

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDO DE OPERAÇÕES TERRESTRES

Manual de Campanha
CONTRAINTELIGÊNCIA

1ª Edição
2019

EB70-MC-10.220



MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDO DE OPERAÇÕES TERRESTRES

Manual de Campanha
CONTRAINTELIGÊNCIA

1ª Edição
2019

PORTARIA Nº 076-COTER, DE 09 DE JULHO DE 2019

Aprova o Manual de Campanha EB70-MC-10.220 - Contraineligência, 1ª Edição, 2019, e dá outras providências.

O **COMANDANTE DE OPERAÇÕES TERRESTRES**, no uso da atribuição que lhe confere o inciso II do art. 16 das INSTRUÇÕES GERAIS PARA O SISTEMA DE DOCTRINA MILITAR TERRESTRE – SIDOMT (EB10-IG-01.005), 5ª Edição, aprovadas pela Portaria do Comandante do Exército nº 1.550, de 8 de novembro de 2017, resolve:

Art. 1º Aprovar o Manual de Campanha EB70-MC-10.220 – Contraineligência, 1ª Edição, 2019, que com esta baixa.

Art. 2º Revogar o Manual de Campanha C-30-3 Contraineligência, 2ª Edição, 2009, aprovado pela Portaria nº 022-EME-Res, de 24 de abril de 2009.

Art. 3º Determinar que esta Portaria entre em vigor na data de sua publicação.

Gen Ex JOSÉ LUIZ DIAS FREITAS
Comandante de Operações Terrestres

(Publicado no Boletim do Exército nº 30, de 26 de julho de 2019)

As sugestões para o aperfeiçoamento desta publicação, relacionadas aos conceitos e/ou à forma, devem ser remetidas para o e-mail portal.cdoutex@coter.eb.mil.br ou registradas no site do Centro de Doutrina do Exército <http://www.cdoutex.eb.mil.br/index.php/fale-conosco>

A tabela a seguir apresenta uma forma de relatar as sugestões dos leitores.

[illegible]

FOLHA REGISTRO DE MODIFICAÇÕES (FRM)

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA

ÍNDICE DE ASSUNTOS

	Pag
CAPÍTULO I – INTRODUÇÃO	
1.1 Finalidade	1-1
1.2 Considerações Gerais	1-1
1.3 Segmentos da Contraineligência	1-4
CAPÍTULO II – AMEAÇAS	
2.1 Conceitos	2-1
2.2 Atores	2-1
2.3 Ação Hostil	2-2
2.4 Motivação	2-3
2.5 Capacidade de Agir	2-4
CAPÍTULO III – SEGURANÇA ORGÂNICA	
3.1 Conceito	3-1
3.2 Concepção	3-1
3.3 Composição	3-2
3.4 Segurança dos Recursos Humanos	3-2
3.5 Segurança do Material	3-4
3.6 Segurança das Áreas e Instalações	3-5
3.7 Segurança da Informação	3-10
3.8 Assessoria Técnica de Contraineligência	3-30
CAPÍTULO IV – SEGURANÇA ATIVA	
4.1 Conceito	4-1
4.2 Concepção	4-1
4.3 Composição	4-1
4.4 Contraespionagem	4-2
4.5 Contraterrorismo	4-4
4.6 Contrassabotagem	4-5
4.7 Contra-ações Psicológicas	4-8
4.8 Contraineligência Interna	4-12

CAPÍTULO V – PLANEJAMENTO DE CONTRAINTELIGÊNCIA

5.1 Considerações Gerais	5-1
5.2 Concepção do Planejamento	5-1
5.3 Condicionantes do Planejamento	5-2
5.4 Fases do Planejamento	5-2
5.5 Exame de Situação	5-3
5.6 Processo de Desenvolvimento da Contrainteligência	5-18

ANEXO A - MEMENTO DO EXAME DE SITUAÇÃO DE CONTRAINTELIGÊNCIA

ANEXO B - PLANO DE SEGURANÇA ORGÂNICA

ANEXO C - PLANO DE CONSCIENTIZAÇÃO

ANEXO D - PLANO DE TREINAMENTO CONTINUADO

ANEXO E - PLANO DE MONITORAMENTO DO PDCI

ANEXO F - MONTAGEM DE LISTAS DE VERIFICAÇÃO

ANEXO G - PROCEDIMENTOS DE MESAS E TELAS LIMPAS

ANEXO H - DECÁLOGO DA CONTRAINTELIGÊNCIA

GLOSSÁRIO

REFERÊNCIAS

CAPÍTULO I

INTRODUÇÃO

1.1 FINALIDADE

1.1.1 O presente manual tem por finalidade estabelecer conceitos e procedimentos referentes à Contrainteligência, bem como orientar os trabalhos de Contrainteligência nas organizações militares (OM) do Exército.

1.2 CONSIDERAÇÕES GERAIS

1.2.1 RAMOS DA INTELIGÊNCIA MILITAR

1.2.1.1 A Inteligência Militar desdobra-se em dois ramos intrinsecamente ligados: o ramo Inteligência e o ramo Contrainteligência.

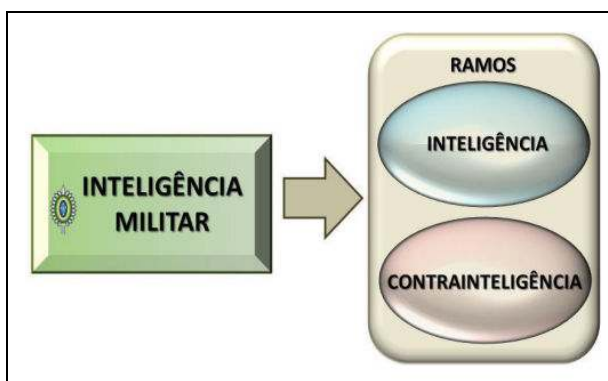


Fig 1-1 Ramos da Inteligência Militar

1.2.2 CONCEITO

1.2.2.1 A Contrainteligência é o ramo da Atividade de Inteligência Militar voltado para prevenir, detectar, identificar, avaliar, obstruir, explorar e neutralizar a atuação da Inteligência adversa e as ações de qualquer natureza que possam se constituir em ameaças à salvaguarda de dados, conhecimentos, áreas, instalações, pessoas e meios que o Exército Brasileiro tenha interesse de preservar.

1.2.3 CONCEPÇÃO DA CONTRAINTELIGÊNCIA NO EXÉRCITO BRASILEIRO

1.2.3.1 A Contrainteligência é um instrumento eficaz do comando em todos os escalões. Suas ações não se restringem ao Sistema de Inteligência do Exército (SIEEx). Ao contrário, cada um dos integrantes do Exército tem responsabilidades para com as atividades e tarefas de proteção da Força. Envolve comportamentos, atitudes preventivas, proatividade e adoção consciente de medidas efetivas.

1.2.3.2 As atividades e tarefas concernentes a esse ramo são desenvolvidas de forma constante e ininterrupta, buscando-se a antecipação diante das potenciais ações hostis contra a Força.

1.2.3.3 A Contrainteligência é dinâmica, necessitando ser constantemente aplicada e retroalimentada, em face da incerteza inerente às ameaças, que estão em constante evolução.

1.2.3.4 A Contrainteligência orienta-se pelo mapeamento dos ativos do Exército (recursos humanos, informação, instalações, material e áreas), pelo levantamento das deficiências na segurança desses ativos e pelas ameaças reais ou potenciais ao Exército.

1.2.3.5 O ramo Contrainteligência, da mesma forma que o ramo Inteligência, produz conhecimentos para o assessoramento do processo decisório.

1.2.3.6 A ação de comando, em todos os níveis, conscientiza e motiva os subordinados quanto à Contrainteligência.

1.2.3.7 A Contrainteligência é, também, uma das atividades da Função de Combate Proteção. Nesse sentido, todas as considerações constantes deste manual, quer sejam de guerra ou não guerra, devem ser observadas durante as operações militares.

1.2.3.8 Na Contrainteligência, considera-se que:

**TUDO DEVE SER PROIBIDO,
EXCETO SE EXPRESSAMENTE PERMITIDO.**

1.2.4 OBJETIVOS DA CONTRAINTELIGÊNCIA

1.2.4.1 São objetivos da Contrainteligência:

a) Impedir que ações hostis de qualquer natureza:

- 1) provoquem danos à integridade física de pessoal militar ou civil;
- 2) comprometam dados, informações, conhecimentos e sistemas a eles

relacionados;

- 3) levem à perda de armamento e outros materiais de emprego militar;
 - 4) inviabilizem a utilização de áreas, instalações e meios de transporte; e
 - 5) atentem contra os valores, os deveres e a ética militar no Exército.
- b) Impedir a realização de atividades de espionagem, sabotagem, ação psicológica hostil, terrorismo ou desinformação.
 - c) Induzir o centro de decisão hostil a posicionar-se de forma equivocada.

1.2.5 ATRIBUIÇÕES DE CONTRAINTELIGÊNCIA

1.2.5.1 Dos Integrantes do Exército Brasileiro

- a) Cumprir as diretrizes, normas, instruções e procedimentos estabelecidos, considerando que as atividades do ramo Contrainteligência, no Exército, não se restringem àquelas desenvolvidas por um pequeno grupo de especialistas, analistas e agentes de Contrainteligência.
- b) Implementar, executar e fiscalizar em sua área de atuação, ininterruptamente, as medidas de Contrainteligência estabelecidas.
- c) Informar ao seu superior imediato toda ação, ou efeito desta, que possa ser considerada como atividade que represente ameaça ao Exército, e que seja de seu conhecimento.

1.2.5.2 Do Comandante, Chefe ou Diretor de OM em Todos os Níveis

- a) Zelar para que seus comandados observem fielmente todas as disposições relativas à Contrainteligência.
- b) Solicitar apoio de elementos especializados de Inteligência, sempre que necessário.
- c) Estabelecer medidas de segurança para salvaguardar os ativos da OM contra ações hostis.
- d) Estimular o desenvolvimento da mentalidade de Contrainteligência nos integrantes da OM.
- e) Designar, em Boletim Interno, um oficial para exercer as funções de Oficial de Contrainteligência e de Segurança Orgânica e um graduado para a função de Auxiliar de Segurança Orgânica da OM. Tais militares não precisam pertencer à Agência de Inteligência e podem elaborar medidas em conjunto com outros militares da OM.

1.2.5.2.1 Neste manual, o Comandante, Chefe ou Diretor de OM, é denominado Comandante.

1.2.5.3 Do Oficial de Contrainteligência e de Segurança Orgânica

- a) Assessorar o Comandante imediato nos assuntos relativos à Contrainteligência.
- b) Identificar as ameaças à OM, observado o Plano de Inteligência do respectivo escalão e as deficiências existentes.
- c) Planejar, coordenar e fiscalizar a implantação e execução das medidas de Contrainteligência.

- d) Propor medidas para gerenciar riscos.
- e) Propor medidas que preservem as operações das forças empregadas.
- f) Orientar os militares de outras especialidades em suas atividades de Contrainteligência.
- g) Prover apoio às OM situadas em sua área de atuação, de acordo com a missão e o escalão considerado.
- h) Propor alterações e aprimoramento nas medidas de Contrainteligência da OM.
- i) Manter atualizado o planejamento de Contrainteligência.
- j) Fiscalizar, auditar e validar as medidas de Contrainteligência a serem adotadas.

1.2.5.4 Do Graduado de Contrainteligência e de Segurança Orgânica

- Auxiliar o Oficial de Contrainteligência e de Segurança Orgânica nas atividades inerentes à Contrainteligência.

1.3 SEGMENTOS DA CONTRAINTELIGÊNCIA

1.3.1 Para racionalização dos trabalhos de Contrainteligência, as ações a serem executadas agrupam-se segundo o caráter preventivo e preditivo que as caracterizam, em dois segmentos distintos:

- a) Segurança Orgânica; e
- b) Segurança Ativa.

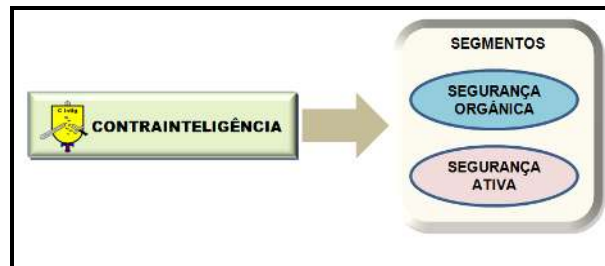


Fig 1-2 Segmentos da Contrainteligência

1.3.2 Enquanto a Segurança Orgânica, em linhas gerais, objetiva proteger os ativos do Exército Brasileiro, a Segurança Ativa visa a atuar contra as ameaças.

1.3.3 A Segurança Ativa está intimamente ligada à Segurança Orgânica, complementando-a e sendo por ela auxiliada.

1.3.4 O Processo de Desenvolvimento da Contraineligência (PDCI) é uma ferramenta que contribui para a efetividade de ambos os segmentos. Ele será tratado, detalhadamente, no Capítulo V.

Desenvolver a mentalidade de Contraineligência é um objetivo que deve ser buscado de forma permanente. A conscientização do público interno contribui para reduzir as deficiências e dificultar a atuação das ameaças.

CAPÍTULO II

AMEAÇAS

2.1 CONCEITOS

2.1.1 Ameaça é a conjunção de ator, motivação e capacidade de realizar ação hostil, real ou potencial, com possibilidade de, por intermédio da exploração de deficiências, comprometer as informações, afetar o material, o pessoal e seus valores, bem como as áreas e instalações, podendo causar danos ao Exército (Fig 2-1).



Fig 2-1 Síntese do Conceito de Ameaça

2.1.2 As ameaças decorrentes de fenômenos naturais, condições técnicas, condições ambientais ou de outra natureza também são consideradas. Por sua especificidade, essas ameaças são uma exceção ao conceito supracitado.

2.1.3 Vulnerabilidade é a deficiência que, ao ser explorada pela ameaça, pode causar incidentes de segurança e gerar impactos negativos para o Exército Brasileiro (Fig 2-2).

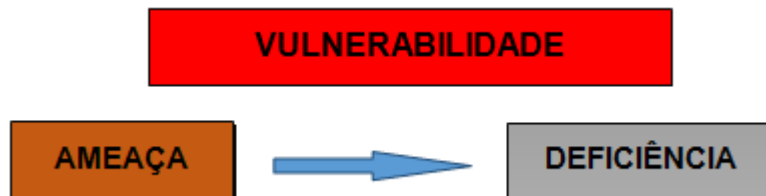


Fig 2-2 Síntese do Conceito de Vulnerabilidade

2.2 ATORES

2.2.1 Os atores a serem considerados, sob o ponto de vista das ameaças, podem ser integrantes do público interno ou externo.

2.2.1.1 O Público Interno é constituído pelos militares da ativa e inativos, ex-combatentes e servidores civis, todos do Exército, bem como, naquilo que couber,

seus dependentes e os alunos dos Colégios Militares.

2.2.1.2 O Público Externo é constituído pelas pessoas, grupos de pessoas ou organizações não incluídos no público interno.

2.3 AÇÃO HOSTIL

2.3.1 Ação, intencional ou não, que possa causar danos aos ativos do Exército.

2.3.2 PRINCIPAIS AÇÕES HOSTIS

2.3.2.1 Ações Contra Instalações Militares

2.3.2.1.1 São exemplos de ações contra instalações militares (ACIM): invasão; tentativa de invasão; disparos de arma de fogo; arremesso de material; arremesso de artefato explosivo; sabotagem; e foto filmagem não autorizada, com ou sem o emprego de aeronaves remotamente pilotadas (ARP) ou drones.

2.3.2.2 Ilícitos Penais e Irregularidades

2.3.2.2.1 Essas ações podem envolver integrantes do público interno como vítimas ou autores.

2.3.2.3 Utilização Indevida de Informações Ostensivas

2.3.2.3.1 As informações de caráter ostensivo, inclusive as disponibilizadas no contexto da Política de Dados Abertos do Exército Brasileiro, podem conter dados passíveis de serem explorados por atores hostis.

2.3.2.3.2 Tais informações podem ser obtidas, por exemplo, em boletins e publicações internas, além das publicações disponibilizadas na internet.

2.3.2.4 Espionagem

2.3.2.4.1 A espionagem visa à obtenção de conhecimento, dado sigiloso, documento ou material para beneficiar estados, grupos de países, organizações, facções, empresas ou indivíduos.

2.3.2.5 Sabotagem

2.3.2.5.1 As ações de sabotagem têm como alvo, basicamente, material, informação, pessoal e instalações.

2.3.2.6 Terrorismo

2.3.2.6.1 A ameaça terrorista pode efetivar-se em ações sobre o pessoal, sistemas de informação, material ou áreas e instalações.

2.3.2.7 Ação Psicológica Hostil

2.3.2.7.1 A ação psicológica hostil orienta seu esforço no sentido de afetar os valores, os deveres e a ética militar.

2.3.2.8 Desinformação

2.3.2.8.1 A desinformação é utilizada para iludir ou confundir um decisor oponente de forma intencional, visando a induzi-lo em erro de avaliação.

2.3.2.9 Ações Hostis no Espaço Cibernético

2.3.2.9.1 A dependência dos sistemas de informação e dos meios de tecnologia da informação e comunicações (MTIC), além das informações neles armazenadas, torna esses ativos alvos compensadores para a execução de ações hostis.

2.3.2.9.2 O comprometimento das redes de computadores e dos sistemas informatizados, normalmente, acontece por meio do uso de *malwares* e da exploração de deficiências de *software*, de *hardware* ou de falha humana.

2.3.2.9.3 Os principais meios de propagação de *malwares* são os dispositivos USB (*pendrives*, HDs externos e outros) infectados, *phishing* e-mails e sites maliciosos ou fraudulentos.

2.3.2.10 Outras ações hostis

2.3.2.10.1 Podem existir outras ações hostis no espaço cibernético capazes de atingir o Exército, tanto pelo emprego de uma forma modificada de ataque quanto pela conjunção de várias modalidades. A principal falha a ser explorada é a humana, implicando atenção especial e permanente.

2.4 MOTIVAÇÃO

2.4.1 É um estado interno que resulta de uma necessidade do ator, dirigindo o comportamento humano para a satisfação dessa necessidade.

2.4.2 Algumas das motivações possíveis são: financeira; ressentimento; vaidade; vingança; estresse; e insatisfação.

2.5 CAPACIDADE DE AGIR

2.5.1 É o potencial de um ator para executar uma determinada ação.

2.5.2 Afirmar que um ator tem capacidade de agir significa dizer que ele pode realizar uma ação. Quanto mais alternativas e liberdade de ação o ator dispuser, maior será a sua capacidade de agir.

2.5.3 A capacidade de agir, combinada com a motivação, é o elo entre o ator e a concretização de sua ação.

2.5.4 Na identificação da capacidade de agir do ator, são considerados os recursos ao seu dispor e a sua habilitação técnica para determinada tarefa, bem como sua liberdade de ação para empregar esses recursos, explorando as deficiências identificadas por ele.

2.5.5 São exemplos de recursos: finanças; equipamentos; documentos; pessoal; conhecimento; habilidade; influência; relação de autoridade; e opinião pública, dentre outros.

CAPÍTULO III

SEGURANÇA ORGÂNICA

3.1 CONCEITO

3.1.1 A Segurança Orgânica é o segmento da Contraineligência que preconiza a adoção de um conjunto de medidas destinado a prevenir e obstruir possíveis ameaças de qualquer natureza dirigidas contra pessoas, dados, informações, materiais, áreas e instalações.

3.2 CONCEPÇÃO

3.2.1 A Segurança Orgânica implica a adoção de postura preventiva por todos os integrantes do Exército, sendo necessária a criação, o desenvolvimento e a manutenção de uma mentalidade de Contraineligência em toda a estrutura hierárquica, visando à obtenção de um grau de proteção ideal.

3.2.2 As medidas de Segurança Orgânica são implementadas mediante criterioso processo, que envolve um ciclo contínuo de planejamento, execução, controle e realimentação.

3.2.3 O cumprimento de regras previstas nos documentos normativos de Segurança Orgânica é responsabilidade de cada integrante do Exército, de acordo com o seu nível de acesso e a sua esfera de atribuições, seja militar ou civil.

3.2.4 O comando enquadrante é o responsável pelo planejamento e pela execução das inspeções ou visitas para verificação do nível de desenvolvimento da Segurança Orgânica, de acordo com as instruções e normas em vigor.

3.2.5 No estabelecimento da Segurança Orgânica, os seguintes aspectos são levados em consideração:

- a) os meios disponíveis;
- b) as deficiências;
- c) as ameaças; e
- d) o grau de segurança ideal a ser obtido.

3.2.6 No que concerne à Segurança Orgânica, normalmente, a segurança é inversamente proporcional ao conforto e à rapidez. Assim, o planejamento pode indicar maior relevância daquela, em detrimento destes, o que ressalta

a importância do desenvolvimento da mentalidade de Contrainteligência.

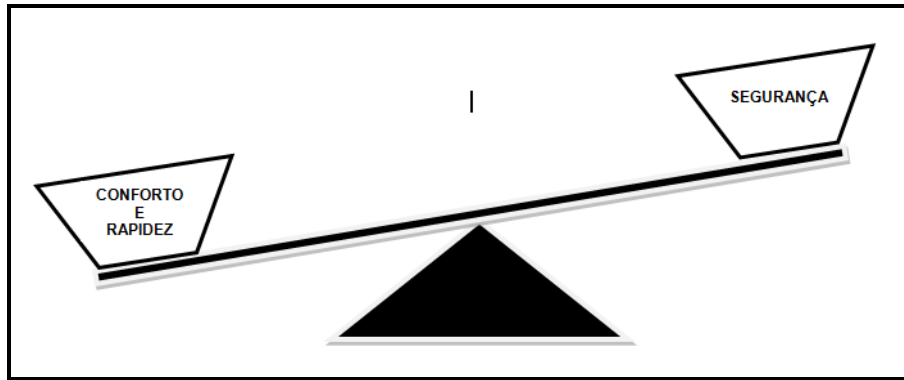


Fig 3-1 Relação segurança x conforto e rapidez

3.3 COMPOSIÇÃO

3.3.1 Para atingir o grau de segurança desejado, a Segurança Orgânica é composta pelos seguintes grupos de medidas:

- a) Segurança dos Recursos Humanos;
- b) Segurança do Material;
- c) Segurança das Áreas e Instalações; e
- d) Segurança da Informação.

3.3.2 Em todos os grupos de medidas da Segurança Orgânica, é necessário considerar a execução de avaliações de riscos para determinar quais os ativos devem ser protegidos, visando a evitar o excesso ou a insuficiência de medidas.

3.3.3 As medidas de Segurança Orgânica devem ser conhecidas, adotadas e praticadas por todos os integrantes do Exército.

3.4 SEGURANÇA DOS RECURSOS HUMANOS

3.4.1 CONCEITO

3.4.1.1 Consiste no grupo de medidas destinadas a preservar a integridade física e moral dos recursos humanos do Exército Brasileiro.

3.4.2 CONSIDERAÇÕES GERAIS

3.4.2.1 Os recursos humanos, bens mais importantes do Exército, precisam ser protegidos e preservados.

3.4.2.2 As ameaças e deficiências, relativas à Segurança dos Recursos Humanos, são consideradas no contexto de uma avaliação da atuação antagônica de atores de qualquer natureza contra o Exército.

3.4.2.3 O sucesso das ações nos assuntos de Segurança dos Recursos Humanos está diretamente associado à conscientização do público interno quanto às prováveis ameaças, bem como ao treinamento e à qualidade das soluções propostas.

3.4.2.4 A permanência por elevado tempo no desempenho de atividades sensíveis representa um risco a ser considerado. Para minimizá-lo, será efetuada, sempre que se mostre possível e necessário, a troca dos militares ou servidores que desempenham essas funções, inclusive os que lidam com a Contrainteligência.

3.4.3 MEDIDAS DE SEGURANÇA DOS RECURSOS HUMANOS

3.4.3.1 A integração eficaz da Segurança Orgânica com a Segurança Ativa permite a antecipação das ameaças e o estabelecimento de medidas adequadas de Segurança dos Recursos Humanos.

3.4.3.2 A fim de assegurar um grau de segurança ideal no que concerne à proteção do pessoal, são adotadas medidas para fazer face às ameaças a esse ativo do Exército, considerando-se:

- a) a possibilidade de envolvimento de integrantes do público interno como vítimas de ilícitos ou irregularidades;
- b) a espionagem, que pode utilizar-se de integrantes do Exército, tanto como agentes infiltrados quanto pela exploração de suas eventuais deficiências;
- c) o terrorismo, que pode afetar a integridade física do pessoal;
- d) a ação psicológica hostil, que pode minar o moral e a disciplina da tropa;
- e) a desinformação, pela possibilidade de influenciar o processo de tomada de decisão;
- f) a ação hostil, que atente contra a integridade física de integrantes do público interno;
- g) os acidentes, de qualquer natureza, que podem causar danos ao pessoal, incluindo-se os fenômenos naturais; e
- h) a produção de conhecimentos e dados estatísticos sobre acidentes, ilícitos penais, disparos acidentais e óbitos.

3.4.3.3 As medidas de Segurança dos Recursos Humanos são estabelecidas, após uma análise minuciosa das ameaças.

3.4.3.4 Dentre as medidas de segurança, destaca-se o exercício da ação de comando, em todos os níveis, com o fim de reforçar, nos integrantes do Exército, os valores éticos e morais que norteiam a Instituição.

3.5 SEGURANÇA DO MATERIAL

3.5.1 CONCEITO

3.5.1.1 Consiste no grupo de medidas voltadas à proteção do material do Exército, de forma direta ou indireta.

3.5.2 CONSIDERAÇÕES GERAIS

3.5.2.1 A Segurança do Material tem importância destacada na prevenção das ações hostis desenvolvidas com o objetivo deliberado de apropriação do material.

3.5.2.2 As ações de sabotagem constituem, também, uma ameaça, podendo provocar a perda do material ou sua indisponibilidade.

3.5.3 MEDIDAS DE SEGURANÇA DO MATERIAL

3.5.3.1 Na avaliação da importância de determinado material, sob o ponto de vista da Segurança Orgânica, é considerado o seu impacto para o cumprimento da missão da OM, bem como sua dificuldade de reposição, entre outros fatores, indicando a necessidade de sua proteção e preservação.

3.5.3.2 As medidas de Segurança do Material abrangem a guarda do material em condições técnicas adequadas e em instalações apropriadas, segundo os manuais técnicos e as possibilidades das ameaças.

3.5.3.3 As ameaças e deficiências, relativas à Segurança do Material, são consideradas no contexto da possibilidade de realização de ação hostil, de qualquer natureza, contra o Exército.

3.5.3.4 O sucesso das ações de Segurança do Material também está diretamente associado à conscientização do público interno, ao treinamento da utilização do material, à qualidade das soluções adotadas e à proteção física contra ameaças internas e externas.

3.5.3.5 Danos ao material podem decorrer de atos não intencionais, ou não, bem como de fenômenos naturais.

3.5.3.6 Os equipamentos e outros materiais relevantes são instalados e protegidos, visando a reduzir os riscos decorrentes de ameaças de qualquer natureza.

3.5.3.7 Em demonstração, exposição ou exibição pública, cabe ao Comandante de OM, por ela responsável, tomar as medidas necessárias de

segurança relativa ao contato de pessoas não integrantes da instituição, com o material sensível exposto, bem como com relação à divulgação das características técnicas.

3.6 SEGURANÇA DAS ÁREAS E INSTALAÇÕES

3.6.1 CONCEITO

3.6.1.1 Consiste no grupo de medidas voltadas para os locais em que ocorram atividades humanas ou nos quais são elaboradas, tratadas, manuseadas ou guardadas informações e materiais, com a finalidade de salvaguardá-los.

3.6.2 CONSIDERAÇÕES GERAIS

3.6.2.1 A Segurança das Áreas e Instalações tem importância destacada na prevenção de ações hostis desenvolvidas com o objetivo deliberado de causar danos ao pessoal, material, patrimônio ou comprometer a informação, particularmente, com atos de espionagem ou sabotagem.

3.6.2.2 Esse grupo de medidas permeia todas as demais atividades de Segurança Orgânica. Para tanto, é importante considerar o assessoramento de Contrainteligência na elaboração de projetos de construção, reforma ou adequação de edificações.

3.6.2.3 A implementação da Segurança das Áreas e Instalações exige o cumprimento de medidas de segurança relativas às áreas, edificações e instalações sob jurisdição do Exército, em particular os locais que contenham informação classificada ou sob restrição de acesso, e os materiais de acesso restrito.

3.6.2.4 As áreas sob controle da OM, permanentes (aquartelamento, campos de instrução etc.) ou temporárias (áreas de instrução, acampamentos, instalações etc.), estão suscetíveis a acidentes, de toda natureza, que podem causar o comprometimento dos demais ativos nelas existentes.

3.6.2.5 Os fenômenos naturais, os acontecimentos fortuitos e os atos praticados (por ação ou omissão), ainda que sem objetivo deliberado de causar danos, também são considerados no que tange à Segurança das Áreas e Instalações.

3.6.3 MEDIDAS DE SEGURANÇA DAS ÁREAS E INSTALAÇÕES

3.6.3.1 Demarcação das Áreas

3.6.3.1.1 Tem por objetivo identificar as áreas de acesso restrito, por meio de sinalizações de fácil entendimento, apresentando-se como um primeiro elemento dissuasor à quebra de segurança.

3.6.3.2 Implementação de Barreiras

3.6.3.2.1 Barreiras são obstáculos, de qualquer natureza, para impedir o ingresso de pessoas não autorizadas nas áreas de acesso restrito e permitir um efetivo controle da circulação das pessoas que possuam autorização para tal.

3.6.3.2.2 As barreiras podem ser físicas (cercas, muros, guardas ou animais) ou conceituais (áreas com acesso restrito, faixas delimitadoras pintadas etc.).

3.6.3.2.3 Principais aspectos considerados na definição das barreiras:

- a) a proteção deve ser compatível com os riscos identificados;
- b) a proteção física pode ser alcançada, por intermédio da criação, se possível, de barreiras sucessivas em torno da área da OM ou de parte de suas instalações, de modo que cada linha de barreira estabeleça um perímetro de segurança;
- c) a localização e a capacidade de cada barreira dependem do Exame de Situação;
- d) qualquer barreira só será efetiva se complementada por outras medidas;
- e
- e) as barreiras e os perímetros adicionais, para controlar o acesso físico, podem ser necessários em áreas com diferentes requisitos de segurança, dentro de um mesmo perímetro.

3.6.3.3 Estabelecimento de Linhas de Proteção

3.6.3.3.1 As linhas de proteção compartimentam ambientes, salas e corredores. Além disso, definem acessos de maior ou menor restrição, para os integrantes dotados de credencial de segurança.

3.6.3.3.2 Sob o aspecto físico, admite-se a necessidade de proteção de áreas e instalações e, ainda, que estas possam estar inclusas em um perímetro de segurança, como um determinado setor de vigilância.

3.6.3.3.3 Podem ser estabelecidas linhas a partir das quais esses locais estarão seguros. Consideram-se, como exemplo, as duas linhas de cercas que, em geral, protegem os paióis.

3.6.3.3.4 Um sistema de detecção pode ser implementado, entre uma linha e outra, para o acionamento dos procedimentos necessários, antes que a ameaça atinja a linha subsequente.

3.6.3.4 Adoção de Controle de Acesso

3.6.3.4.1 É um processo que seleciona o acesso de pessoas a qualquer área ou objeto específico.

3.6.3.4.2 Tem por objetivo prevenir o comprometimento das informações e instalações físicas da OM. Para isso, os recursos e as instalações são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras apropriadas e controle de acesso.

3.6.3.4.3 As áreas de segurança devem ser protegidas por controles de entrada apropriados, de modo a assegurar que apenas pessoas autorizadas tenham acesso.

3.6.3.4.4 O controle de acesso baseia-se na identificação e na avaliação dos graus de autorização de entrada e saída, sendo feito, normalmente, por meio de uma ou mais das seguintes medidas:

- a) uso de meios adequados pela pessoa que pretenda acessar a área ou instalação, tais como chave, crachá, cartão magnético ou símbolo;
- b) uso de senha ou código;
- c) identificação de partes físicas do corpo humano (íris, digitais, entre outras); e
- d) combinação desses meios.

3.6.3.4.5 Os sistemas de controle de acesso variam, desde fechaduras até dispositivos que realizam análises biométricas, passando por uma infinidade de sistemas baseados em cartões, teclados digitais e *scanners*.

3.6.3.5 Emprego de Normas e Procedimentos Adicionais de Segurança

3.6.3.5.1 Normas e procedimentos adicionais são usados para melhorar as condições de segurança das áreas de acesso restrito. Isso inclui controles para o pessoal da OM, para terceiros que trabalham em áreas de acesso restrito, assim como para atividades terceirizadas, que possam ocorrer nessa área.

3.6.3.5.2 Os seguintes itens são considerados:

- a) conhecimento, pelos integrantes da OM, da existência de área de segurança ou que permita atividades dentro dela apenas quando necessário;
- b) evitar o trabalho sem supervisão nas áreas de segurança;
- c) fechamento físico e fiscalização periódica das áreas de segurança

desocupadas;

d) restrição de acesso do pessoal de serviço às áreas de segurança, sendo autorizado somente quando as atividades o exigirem. Esse acesso também deve ser monitorado; e

e) proibição do uso de equipamentos fotográficos, de vídeo, de áudio ou de outro equipamento de gravação, particularmente telefone celular, em qualquer área ou atividade da OM. As autorizações eventuais para emprego desses aparelhos são submetidas à criteriosa análise, considerando a necessidade e a segurança.

3.6.3.6 Detecção de Intrusão e Monitoramento de Alarme

3.6.3.6.1 Os sistemas destinados a detectar intrusão ou violação possuem três elementos básicos, a saber:

- a) dispositivos de detecção - sensores para indicar a presença de intrusos;
- b) sistemas de transmissão - métodos utilizados para transmitir um sinal de alarme; e
- c) sistema de monitoramento - equipamentos usados para registrar acessos e, particularmente, inibir as intrusões.

3.6.3.6.2 Tais equipamentos funcionam, entre outros, com sensores infravermelhos, micro-ondas, ultrassons, deslocamentos de imagens, fotoelétricos, de proximidade, sísmicos, ondas de choque ou a combinação de mais de um deles.

3.6.3.7 Estabelecimento de Segurança em Ambientes Fechados

3.6.3.7.1 Uma área de segurança pode ser caracterizada por um ambiente fechado ou diversas salas, dentro de um perímetro de segurança física. É possível que essa área contenha armários fechados ou cofres.

3.6.3.7.2 A seleção e o projeto de uma área de segurança levam em consideração as possibilidades de ocorrência de danos (causados por fogo, inundações, explosões e outras formas de desastres naturais ou antrópicos), assim como as regulamentações e padrões de segurança e saúde.

3.6.3.7.3 Os seguintes controles são considerados:

- a) as instalações críticas de acesso restrito são localizadas de forma a evitar o acesso indevido;
- b) os serviços de suporte e de equipamentos (fotocopiadoras, por exemplo) são instalados de forma a evitar acesso que possa vir a comprometer a proteção da informação;
- c) quando não utilizadas, as portas e janelas são fechadas, dispondo de proteção externa (grades), principalmente, se localizadas em andar térreo;
- d) os sistemas de detecção de intrusão são instalados por profissionais

especializados, devidamente identificados, sendo testados periodicamente, de forma a abranger todas as portas externas e janelas acessíveis;

e) as áreas, quando não ocupadas por pessoal, possuem sistema de alarme que permanece ativado constantemente;

f) as instalações de processamento da informação, gerenciadas pela OM, são separadas fisicamente das que estejam sob responsabilidade de terceiros;

g) o acesso aos arquivos e listas de telefones internos, que identificam os locais e o pessoal que lida com atividades sensíveis, é restrito;

h) os materiais combustíveis ou perigosos são guardados de forma segura, inclusive no que tange à distância apropriada de ativos a serem protegidos;

i) os suprimentos volumosos não devem ser guardados em uma área de segurança, exceto se isso for imprescindível; e

j) os materiais de contingência e meios magnéticos de reserva (*backup*) são guardados a uma distância segura da instalação principal para evitar a sua destruição por desastres ocorridos neste local.

3.6.3.8 Isolamento das Áreas de Expedição e de Carga

3.6.3.8.1 Essas áreas, normalmente, recebem pessoas externas à OM, sendo controladas e, se possível, isoladas das áreas de acesso restrito.

3.6.3.8.2 Os requisitos de segurança são determinados a partir de uma análise de risco.

3.6.3.9 Emprego de Equipamentos de Segurança

3.6.3.9.1 Equipamentos de segurança, tais como os equipamentos de combate a incêndio, são instalados com o objetivo de se prevenir perda, dano ou comprometimento dos ativos e a interrupção das atividades da OM.

3.6.3.9.2 Os equipamentos são protegidos fisicamente de ameaças à sua segurança e de perigos ambientais. Controles especiais podem ser exigidos para salvaguardar as instalações de infraestrutura, como o fornecimento de energia elétrica e cabeamento.

3.6.3.10 Estabelecimento de Proteção Elétrica

3.6.3.10.1 Todos os equipamentos elétricos devem ser protegidos contra falhas de energia e outras anomalias na alimentação elétrica.

3.6.3.10.2 Algumas medidas para evitar cortes ou falhas no fornecimento elétrico incluem alimentação múltipla, *nobreak* ou gerador. Essas ações objetivam a continuidade na operação dos sistemas elétricos e eletrônicos.

3.6.3.10.3 É necessário que os interruptores elétricos estejam localizados próximos às saídas de emergência das salas de equipamentos, de modo a facilitar o desligamento em caso de necessidade.

3.6.3.10.4 A iluminação de emergência deve estar disponível em casos de falha na fonte elétrica primária.

3.6.3.10.5 É necessário que a proteção contra raios seja usada em todos os prédios; e que filtros de proteção contra raios sejam instalados em todas as linhas de comunicação externas.

3.6.3.11 Proteção do Cabeamento

3.6.3.11.1 Todo o cabeamento elétrico e de telecomunicação que transmite dados, ou suporta os serviços de informação, deve ser protegido contra interceptação ou danos.

3.6.3.11.2 As seguintes ações devem ser consideradas:

- a) proteger o cabeamento da rede contra interceptações ou danos;
- b) separar os cabos elétricos e os cabos de comunicação, para prevenir interferências;
- c) instalar conduítes blindados e salas ou gabinetes trancados nos pontos de inspeção e terminais;
- d) usar rotas e meios de transmissão alternativos;
- e) instalar cabeamento de fibra óptica;
- f) realizar varreduras periódicas, para identificar dispositivos não autorizados conectados aos cabos; e
- g) tornar subterrâneas as linhas elétricas e de telecomunicações das instalações de processamento da informação ou submetê-las à proteção alternativa adequada.

3.7 SEGURANÇA DA INFORMAÇÃO

3.7.1 CONCEITO

3.7.1.1 A Segurança da Informação consiste no grupo de medidas destinado a garantir a disponibilidade, integridade, confidencialidade (sigilo), autenticidade, irretratabilidade (não repúdio) e atualidade da informação, em todo o seu ciclo de vida.

3.7.2 CONSIDERAÇÕES GERAIS

3.7.2.1 A Informação é um recurso vital para o adequado funcionamento de toda e qualquer OM, sendo tratada como ativo a ser protegido.

3.7.2.2 A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, mostrada em filmes ou difundida verbalmente. Seja qual for a sua forma, ou o meio pelo qual é compartilhada ou armazenada, é necessário que a informação seja protegida.

3.7.2.3 Dessa forma, a Segurança da Informação atua objetivamente sobre os suportes da informação, que são as pessoas, os documentos, os materiais, os MTIC, as áreas e as instalações.

3.7.2.4 A Segurança da Informação é obtida a partir da implementação de uma série de controles estabelecidos para garantir que os objetivos de segurança específicos sejam atendidos.

3.7.2.5 A Segurança da Informação deve estar em conformidade com os requisitos legais e as normas internas do Exército. Ressalte-se a importância dos direitos de propriedade intelectual, proteção de dados, privacidade da informação pessoal e prevenção do uso indevido de facilidades de processamento da Informação.

3.7.2.6 Visando a prover o adequado nível de Segurança da Informação, destaca-se que as Instruções Gerais para Salvaguarda de Assuntos Sigilosos - IGSAS (EB10-IG-01.011) regulam o acesso, a divulgação e o tratamento de informações sigilosas no âmbito do Exército.

3.7.3 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

3.7.3.1 A Segurança da Informação é caracterizada pela preservação dos seguintes princípios:

- a) Confidencialidade (sigilo) - garantia de que o conteúdo da informação só é acessível e interpretável por quem possuir autorização;
- b) Integridade - garantia de que o conteúdo original da informação não seja modificado; é a certeza de que a exatidão e a inteireza estejam salvaguardadas;
- c) Disponibilidade - garantia de que o conteúdo da informação esteja disponível para quem possuir autorização ou credencial de segurança, sempre que houver necessidade;
- d) Autenticidade - certificação de que o conteúdo da informação possua integridade, assim como a fonte geradora tenha sua origem comprovada;
- e) Inviolabilidade - garantia de que os meios de proteção da informação não sejam violados; e
- f) Irretratabilidade (não repúdio) - garantia de que, num processo de envio e recebimento de informações, qualquer participante, originador ou destinatário de informação, não possa, em um momento posterior, negar a respectiva atuação.

3.7.4 REGRAS GERAIS DA SEGURANÇA DA INFORMAÇÃO

3.7.4.1 A Segurança da Informação está diretamente associada à conscientização do público interno, à capacitação dos recursos humanos e à qualidade das soluções adotadas para a proteção das informações.

3.7.4.2 As ameaças e as deficiências, relativas à segurança dos dados e informações, são consideradas no contexto da crescente informatização de atividades e processos.

3.7.4.3 Para a otimização da Segurança da Informação, pode ser necessária a participação de outros agentes, como a contratação de consultoria externa especializada ou a realização de assessoria técnica, por órgão do Exército.

3.7.4.4 A adoção de qualquer solução tecnológica, nacional ou estrangeira, para atendimento a requisitos relativos à Segurança da Informação, no âmbito do Exército, é precedida de estudos sobre a sua pertinência, confiabilidade, permanência, manutenção e suporte.

3.7.4.5 A compartimentação de funções contribui para a redução dos riscos para a segurança da informação, inclusive no que se refere aos sistemas e MTIC.

3.7.4.6 São avaliados os riscos decorrentes do acesso de terceiros a dados e informações sensíveis, inclusive aos seus suportes.

3.7.4.7 É necessário que os requisitos de segurança resultantes do acesso de terceiros (incluindo os prestadores de serviço que trabalhem na OM) constem nos contratos firmados, particularmente, no que tange à assinatura do Termo de Compromisso de Manutenção do Sigilo (TCMS).

3.7.5 CLASSIFICAÇÃO E CONTROLE

3.7.5.1 Classificação é o ato de se atribuir grau de sigilo à informação que requeira medidas especiais de salvaguarda e, por consequência, aos seus suportes.

3.7.5.2 A informação é classificada para indicar sua importância, prioridade e tratamento.

3.7.5.3 Um conjunto de medidas é definido para rotular e tratar a informação, de acordo com o processo de classificação adotado pelo Exército. Esses procedimentos precisam abranger tanto a informação no formato físico quanto no digital.

3.7.5.4 Para cada classificação, é necessário que procedimentos de tratamento sejam definidos para abranger os seguintes tipos de atividade de processamento da informação:

- a) produção;
- b) cópia e manuseio;
- c) armazenamento;
- d) transmissão; e
- e) eliminação.

3.7.6 COMPOSIÇÃO DA SEGURANÇA DA INFORMAÇÃO

3.7.6.1 A Segurança da Informação compreende os seguintes subgrupos de medidas:

- a) Segurança da Informação no Pessoal;
- b) Segurança da Informação na Documentação;
- c) Segurança da Informação no Material;
- d) Segurança da Informação nos Meios de Tecnologia da Informação e Comunicações; e
- e) Segurança da Informação nas Áreas e Instalações.

3.7.6.2 Segurança da Informação no Pessoal

3.7.6.2.1 Consiste no subgrupo de medidas destinadas a assegurar comportamentos, no público interno, adequados à proteção de dados e informações de natureza institucional.

3.7.6.2.2 A Segurança da Informação no Pessoal é baseada nas seguintes premissas:

- a) a necessidade de conhecer está ligada à função desempenhada;
- b) o acesso à informação sensível é permitido apenas às pessoas que tenham necessidade de conhecer;
- c) o acesso às informações classificadas, ou sob restrição de acesso, é permitido apenas às pessoas credenciadas ou que tenham assinado o TCMS; e
- d) o conhecimento de assunto sensível depende da função; e não do grau hierárquico.

3.7.6.2.3 São implementadas ações com o objetivo de desenvolver a mentalidade de Contraineligência no público interno, inclusive os servidores civis, com foco na Segurança da Informação.

3.7.6.2.4 Para efeito de sua aplicação, as medidas de Segurança da Informação no Pessoal estão agrupadas em Segurança no Processo Seletivo, no Desempenho da Função e no Desligamento.

3.7.6.2.5 Medidas de Segurança no Processo Seletivo - visam a dificultar a infiltração e a admissão de indivíduos com potencial para comprometer a segurança de dados e informações. Medidas a serem executadas:

- a) avaliação da sensibilidade da função - essa medida é tomada tendo em vista que as diversas funções exercidas nas OM, particularmente na 2ª Seção, possuem um grau de sensibilidade decorrente do valor dos ativos a elas atinentes. Em decorrência dessa avaliação, são determinadas as características pessoais julgadas necessárias para o desempenho dessas funções, sob o ponto de vista da Contraineligência; e
- b) investigação de segurança - essa medida visa a assegurar que os recursos humanos selecionados possuam os atributos necessários para o desempenho das funções consideradas sensíveis.

3.7.6.2.6 Medidas de Segurança no Desempenho da Função - visam a validar o credenciamento, proceder à educação de segurança e confirmar as características pessoais exigidas. Problemas pessoais e financeiros, mudanças de comportamento ou estilo de vida, ausências frequentes e sinais de estresse ou depressão podem levar a fraudes, roubos, erros ou outros riscos. Medidas a serem executadas:

- a) credenciamento de segurança - confirmadas as exigências de segurança inerentes à função, é expedida a credencial de segurança apropriada, por meio de ato administrativo exarado por autoridade competente, estabelecendo o grau de sigilo a que o credenciado poderá ter acesso. Essa credencial de segurança pode ser alterada em função de novas necessidades relativas à mesma função ou outra para a qual o servidor for designado;
- b) educação de segurança - é necessário que os integrantes da OM (militares ou civis) sejam treinados nos procedimentos de segurança e no uso correto das instalações de processamento da informação;
- c) assinatura do TCMS - o acesso de militar ou civil a documento ou material sob restrição de acesso exige a assinatura de TCMS, conforme a necessidade de conhecer e de acordo com o modelo estabelecido pelas IGSAS; e
- d) resposta aos incidentes de segurança e ao mau funcionamento - os incidentes que afetam a segurança são notificados, por meios de canais apropriados, o mais rapidamente possível. Todos os integrantes da OM são orientados a notificarem eventuais incidentes que possam gerar impactos na segurança. Esses incidentes devem ser registrados e informados ao escalão superior, inclusive no âmbito do SIEx, visando ao aprimoramento da segurança.

3.7.6.2.7 Medidas de Segurança no Desligamento

- a) A segurança no desligamento visa a salvaguardar informações sigilosas, após o desligamento, e a garantir a adequada desmobilização.
- b) Os TCMS ficam arquivados, normalmente, na Seção de Inteligência da OM, após o desligamento, por tempo indeterminado, estendendo as responsabilidades pela Segurança da Informação.

3.7.6.3 Segurança da Informação na Documentação

3.7.6.3.1 A Segurança da Informação na Documentação consiste no subgrupo de medidas aplicadas à documentação, destinadas a evitar o seu comprometimento, visando à salvaguarda de dados, informações ou conhecimentos, de caráter sigiloso ou não, que devam ser protegidos.

3.7.6.3.2 Os documentos, historicamente, constituem o suporte mais comum das informações, tornando-se alvos permanentes das ações hostis, em particular da espionagem e da sabotagem.

3.7.6.3.3 O comprometimento pode ocorrer, ainda, em decorrência de fenômenos naturais e, até mesmo, por ações executadas sem objetivo deliberado de afetar a informação.

3.7.6.3.4 Os documentos possuem um ciclo de vida que pode ser desdobrado nas seguintes etapas: produção; expedição; recepção; manuseio; arquivamento; e eliminação.

a) **Segurança na Produção** - as medidas de segurança na produção visam à atribuição de grau de sigilo, ao controle dos recursos utilizados na produção de documentos sigilosos e à marcação desses documentos com sinais de segurança (paginação, autenticação, marca d'água etc.). Medidas a serem executadas:

1) atribuição preliminar de restrição de acesso - atribuir essa restrição ao documento ou material em fase de produção, levando em consideração fatores como natureza do assunto, finalidade, usuário e aspectos essenciais nele contidos;

2) controle dos recursos utilizados - recursos utilizados na elaboração de documentos sigilosos, tais como rascunhos, notas, carbonos e desenhos, são objeto de controle de segurança pelos seus responsáveis. Normalmente, esses recursos são destruídos após a sua utilização ou, quando não for o caso, são objeto de cuidados especiais relativos à sua segurança;

3) numeração das páginas - visa a contribuir para a integridade do documento, representando um sinal de segurança contra o extravio e a subtração de páginas;

4) classificação - tem por objetivo proteger a informação que requeira medidas especiais de salvaguarda, atribuindo-lhe grau de sigilo. A decisão de classificar a informação é formalizada pela emissão de Termo de Classificação de Informação (TCI); e

5) restrição de acesso - será mantido sob restrição de acesso, independentemente de classificação, o documento, a área ou a instalação sob custódia do Exército, de acordo com o estabelecido pelas IGSAS.

b) **Segurança na expedição e na recepção** - as medidas de segurança na expedição e na recepção visam a estabelecer controles de segurança na tramitação dos documentos. Medidas a serem executadas:

1) autenticação de documento - processo utilizado para confirmar ou garantir

ao usuário a identidade de uma pessoa ou organização, garantindo a fidelidade da fonte e confirmando a procedência da documentação;

2) acondicionamento do documento - estabelecimento de procedimentos adicionais de segurança do documento a ser expedido, de modo a dificultar as ações hostis, permitindo a identificação de indícios de eventual comprometimento;

3) controle de saída - adoção de registros de saída, atribuindo-se responsabilidades pela expedição e pelo tráfego do documento sigiloso, para possibilitar o eficaz controle da difusão. Especial atenção merece o endereçamento dos documentos, o qual é antecipadamente confirmado; e

4) controle de entrada - adoção de controles da recepção e tramitação interna dos documentos sigilosos recebidos. Envolve procedimentos relativos à inspeção do acondicionamento e à autorização para abertura de invólucros, assinatura de recibos, distribuição interna, abrangendo todos os tipos de registros que possibilitem a apuração de responsabilidades, quando da constatação de comprometimento.

c) **Segurança no manuseio** - as medidas de segurança no manuseio visam a estabelecer procedimentos para reprodução, custódia e classificação, desclassificação ou reclassificação de documentos sigilosos, permitindo implementar controles de segurança, durante sua utilização. Medidas a serem executadas:

1) controle de reproduções - a cópia ou o extrato de documento classificado ou sob restrição de acesso receberá um código numérico ou alfanumérico específico (controle de vazamento) para cada destinatário, a fim de identificar a origem de um possível vazamento e facilitar o seu controle. Esse código será colocado no corpo do texto, em todas as páginas do documento, sendo visível e de fácil identificação, conforme modelo constante das IGSAS. No documento original, constará a relação de todos os destinatários com os seus respectivos códigos;

2) controle de custódia - enquanto o documento sigiloso permanecer com o usuário, são estabelecidos procedimentos cautelares visando ao seu efetivo controle;

3) classificação, desclassificação ou reclassificação - conforme estabelecido na legislação vigente; e

4) seleção dos documentos a serem arquivados ou eliminados - para determinação da destinação final dos documentos, será observada a legislação vigente.

d) **Segurança no arquivamento** - as medidas de segurança no arquivamento visam a definir os locais e processos adequados de arquivamento e recuperação dos documentos sigilosos e estabelecer rotinas para situações de emergência. Medidas a serem executadas:

1) escolha do local - selecionar o local adequado, sob o enfoque de segurança, para a instalação dos arquivos que abrigam documentos sigilosos. Entre outras, impõem-se as providências quanto à circulação de pessoas e ao deslocamento da documentação em casos de emergência;

2) escolha do tipo de arquivo ou cofre - o tipo de arquivo ou cofre decorre da

avaliação do modelo adequado para abrigar os documentos de diferentes graus de sigilo;

3) controle no arquivamento e na recuperação - é efetivado pelo estabelecimento de rotinas para o arquivamento e a recuperação dos documentos nos arquivos. Exige-se a definição de responsabilidades para o manuseio e controle dos documentos sigilosos arquivados; e

4) estabelecimento de rotinas para evacuação em situações de emergência (medidas de contingência) - são instituídos procedimentos relativos à evacuação da documentação sensível, em situações de emergência. Essas medidas envolvem o estabelecimento de prioridades e responsabilidades e a determinação, antecipada, de locais alternativos para abrigar os documentos a serem salvos.

e) **Segurança na eliminação** - as medidas de segurança na eliminação visam, depois de cumprido o ciclo de vida do documento, de acordo com a legislação em vigor, a definir meios e locais de eliminação, a determinar formas de controle, bem como estabelecer rotinas de eliminação para situações de emergências (medidas de contingência). Medidas a serem executadas:

1) escolha dos meios (material e pessoal) e dos locais a serem utilizados para a eliminação;

2) controle da eliminação - objetiva estabelecer rotinas criteriosas para a efetiva eliminação dos documentos sigilosos julgados inservíveis. Todos os procedimentos são controlados e executados de forma centralizada, a fim de evitar desvios de documentos e falhas no processo que não resultem na sua plena eliminação. Exigem-se providências referentes a relações ou termos de eliminação, obedecendo às prescrições contidas na legislação específica; e

3) estabelecimento de rotinas para eliminação em situações de emergência - visa a evitar a captura de documentos sensíveis pelo inimigo, em situação de combate.

3.7.6.4 Segurança da Informação no Material

3.7.6.4.1 A Segurança da Informação no Material consiste no subgrupo de medidas voltadas para proteger as informações contidas em determinados materiais.

3.7.6.4.2 Para a Segurança da Informação no Material, toda matéria, substância ou artefato que contenha, utilize ou veicule informações, que, de posse de ator(es) de qualquer natureza, possam implicar riscos para qualquer ativo do Exército devem ser salvaguardados.

3.7.6.4.3 O material, em razão da sensibilidade das informações nele contidas, pode tornar-se alvo permanente das ações hostis, em particular da espionagem e da sabotagem.

3.7.6.4.4 O comprometimento pode ocorrer, ainda, em decorrência de fenômenos naturais ou de ações desenvolvidas sem objetivo deliberado de afetar a informação contida no material.

3.7.6.4.5 Com relação à Segurança da Informação no Material, controlado ou não, são adotadas, no que for aplicável, prescrições similares às da Segurança da Informação na Documentação.

3.7.6.4.6 A Segurança da Informação no Material é executada, prioritariamente, por intermédio do cumprimento de regulamentos, instruções ou normas que regem a produção, a classificação, a distribuição, o recebimento, o registro, o manuseio, a guarda, o armazenamento e acondicionamento e a eliminação de materiais.

3.7.6.4.7 Regulamentos específicos devem estabelecer as medidas necessárias à salvaguarda de materiais sigilosos e à segurança na celebração de contratos e convênios, no transporte e na eliminação.

3.7.6.4.8 Segurança de material em trânsito – o material classificado ou sob restrição de acesso pode ficar vulnerável à quebra de segurança, uso impróprio ou alteração, durante o seu transporte físico. Recomenda-se que os seguintes controles sejam aplicados para salvaguardar materiais que estão sendo transportados entre localidades:

- 1) utilização de transporte ou de serviço de mensageiro confiável;
- 2) embalagem adequada para proteger o conteúdo contra qualquer dano físico que possa vir a ocorrer durante o transporte e estar de acordo com especificações dos fabricantes; e
- 3) adoção de controles especiais, quando necessário, para proteger informações sensíveis. Como exemplo, pode-se incluir:
 - utilização de recipientes lacrados (com controle de número de lacre);
 - entrega em mão (com controle de recebimento);
 - utilização de lacre externo de pacotes (que revele qualquer tentativa de acesso);
 - divisão do conteúdo para mais de uma entrega e expedição por rotas distintas em casos excepcionais; e
 - uso de assinatura digital e de criptografia.

3.7.6.4.9 Segurança de equipamentos fora das instalações

- a) O uso de qualquer equipamento que contenha informação sensível, fora das instalações da OM, será previamente avaliado e autorizado.
- b) O grau de segurança será, no mínimo, equivalente àquele existente nas instalações da OM (aquartelamento) para o mesmo propósito.
- c) Os riscos de segurança, tais como dano, roubo e espionagem, podem variar em virtude da localização, impondo o emprego de controles apropriados.

3.7.6.4.10 Reutilização e alienação segura de equipamentos

- a) A Informação pode ser exposta pelo descuido na alienação ou reutilização de equipamentos e materiais.
- b) É necessário que dispositivos de armazenamento e materiais que contenham informação sensível sejam destruídos, fisicamente ou sobrescritos de forma segura, ao invés da utilização de funções-padrão para o apagamento.
- c) Dispositivos de armazenamento danificados que contenham informação sensível podem necessitar de uma análise para determinar a sua eliminação.

3.7.6.4.11 Remoção de propriedade

- a) Equipamentos, informações ou *softwares* não devem ser retirados da OM sem autorização.
- b) São realizadas inspeções de forma a detectar a remoção não autorizada de propriedade. Todos devem estar cientes de que essas inspeções serão realizadas.

3.7.6.5 Segurança da Informação nos MTIC

3.7.6.5.1 A Segurança da Informação nos MTIC consiste no subgrupo de medidas destinadas a salvaguardar as informações, bem como a integridade dos sistemas e MTIC do Exército.

3.7.6.5.2 A Informação é um dos ativos mais valiosos de uma organização. Grande parte dela está armazenada e é transmitida por meios eletrônicos, em um ambiente complexo, exigindo normas de segurança compatíveis, tais como senhas, sistemas de autenticação e criptografia.

3.7.6.5.3 Toda informação classificada ou sob restrição de acesso, que seja armazenada, processada ou trafegue por ambientes de rede de dados é submetida a processos que assegurem a sua disponibilidade, integridade, confidencialidade e autenticidade.

3.7.6.5.4 No planejamento de Segurança da Informação nos MTIC é considerada a capacidade da busca dos atores hostis para obtenção de informações. A busca de dados, informações ou conhecimento exige, além das capacidades de interceptação e armazenamento, capacidade de análise de grande volume de dados, bem como o desenvolvimento de técnicas de criptoanálise.

3.7.6.5.5 Em virtude da crescente importância dos sistemas de TIC para o Exército, impõe-se a adoção de medidas de segurança físicas, de acesso, de conteúdo, de transmissão e de pessoal.

3.7.6.5.6 Essas medidas são aplicadas para que as informações se mantenham íntegras, confiáveis e disponíveis.

3.7.6.5.7 As medidas de prevenção são: conhecer as possíveis formas de ataque; buscar a assinatura das listas de segurança; utilizar programas antivírus atualizados e ferramentas de segurança confiáveis; manter o pessoal treinado e atualizado; selecionar o pessoal criteriosamente; e manter mais de um administrador do sistema.

3.7.6.5.8 A segurança contra ações hostis abrange, também, as medidas de proteção funcional (treinamento e motivação), administrativas (auditoria e fiscalização), de mídia (inspeção, eliminação, armazenamento, uso e contingência), contra radiação (por intermédio do uso de blindagem) e controle de ciclos (registro de ocorrências e reavaliação das medidas de segurança).

3.7.6.5.9 Medidas de segurança física da informação nos MTIC

a) As medidas de segurança de controle físico visam a proteger o ambiente e os locais onde se encontram os meios de TIC, contra o acesso de pessoas não autorizadas, bem como protegê-los dos riscos naturais ou intencionais.

b) Além das medidas de Seg A Inst, são observados, de forma particular, os seguintes procedimentos:

1) armazenagem externa de dados (backup):

- visa a evitar a interrupção do processamento de dados nos casos de sinistro ou sabotagem dos dados originais; e

- o local de armazenagem é afastado do arquivo original, de forma a impossibilitar a sua eliminação simultânea.

2) para a preservação da integridade dos dispositivos durante o transporte, são adotadas as seguintes providências:

- prevenir choques térmicos, choques físicos e desmagnetização;

- utilizar meios adequados de transporte; e

- usar malas adequadas, com divisões internas variadas, que sejam protegidas contra choques e radiações.

3) manutenção de MTIC:

- é executada pelo pessoal especializado da própria OM, preferencialmente;

- esgotados os meios da OM para a resolução de problema de manutenção, a empresa eventualmente contratada ficará submetida ao previsto nas IGSAS;

- qualquer serviço a ser executado em equipamento informatizado por empresa contratada, que contenha assunto classificado ou sob restrição de acesso, será acompanhado pelo responsável por sua utilização; e

- o computador que contenha informação classificada ou sob restrição de acesso e que necessite de manutenção fora da OM terá o seu disco rígido retirado e guardado em um cofre.

3.7.6.5.10 Segurança de *software* e de sistemas

a) Entre os principais tipos de *softwares* estão os de sistema operacional, processador de texto, gerenciador de banco de dados, editoração eletrônica, processador gráfico, planilhas eletrônicas e os corporativos.

b) Ao serem instalados nos equipamentos, os *softwares* possibilitam a

interação do usuário com a máquina, por intermédio do sistema implantado, possuindo, na maioria das vezes, pontos críticos de entrada e, até mesmo, de adequados procedimentos relativos a senhas.

c) As medidas de segurança de *software* são adotadas ou exploradas nos diferentes *softwares*, para que eles não tenham seus códigos-fonte alterados, instalados ou operados por elementos não credenciados.

d) São utilizados apenas *softwares* licenciados, de acordo com a legislação em vigor, inclusive os de domínio público, após parecer favorável e assessoramento técnico de pessoal especializado da OM.

e) A instalação de *software* somente é realizada por pessoal habilitado da OM.

f) O uso de dispositivos móveis, para o trato de informação sensível, é evitado. Caso esse uso seja imprescindível, são adotadas medidas de segurança adicionais (criptografia, uso de contêineres seguros etc.).

3.7.6.5.11 Medidas de segurança de acesso à informação nos meios de TIC

a) É necessário que os acessos à informação e aos processos da OM sejam controlados por meio de normas de segurança, levando-se em consideração as regras para autorização e difusão da informação.

b) As regras de controle de acesso e de direitos, para cada usuário ou grupo de usuários, são claramente estabelecidas.

c) O gerenciamento de acessos do usuário aos sistemas de informação proporciona, no mínimo:

1) registro de usuário (procedimento formal de registro e cancelamento de usuário para obtenção de acesso) e definição das suas responsabilidades;

2) gerenciamento de privilégios, pelo controle de níveis de acesso ao sistema ou aplicação;

3) gerenciamento de senha dos usuários;

4) controle de acesso à rede;

5) compartimentação do acesso, permitindo que os usuários acessem apenas os serviços especificamente autorizados;

6) rota de rede obrigatória entre o terminal do usuário e o serviço do computador;

7) autenticação para conexão externa do usuário e de nó;

8) controle de conexões de rede e proteção de portas de diagnóstico remotas; e

9) compartimentação (segmentação) de redes.

d) Os computadores são configurados para encerrar automaticamente as sessões, por meio de "tempo limite de sessão".

e) O acesso aos computadores é protegido por meio de protetor de tela e senha.

f) Os requisitos das normas de controle de acesso para redes compartilhadas, especialmente aquelas que se estendem além dos limites da OM, podem requerer a incorporação de controles que limitem a capacidade de conexão dos usuários. Tais controles podem ser implementados por meio de *firewall* de rede, que filtram o tráfego usando

tabelas ou regras predefinidas. Entre as redes que necessitam de restrições, destacam-se as aplicações de correio eletrônico, as de transferência unidirecional e bidirecional de arquivos, as de acesso interativo e as que permitem o acesso de acordo com a hora.

g) O acesso às redes de computadores é protegido com a utilização de usuários e senhas, possibilitando a segregação de acesso às informações.

h) As funcionalidades de segurança dos sistemas são usadas para restringir o acesso aos recursos computacionais e às informações. É necessário que estas funcionalidades permitam:

- 1) identificação, autenticação e verificação da identidade e, se necessário, do terminal e da localização de cada usuário autorizado;
- 2) registro dos sucessos e das falhas de acesso ao sistema;
- 3) fornecimento de meios apropriados para a autenticação - se um sistema de gerenciamento de senhas for usado, é necessário que ele garanta o cadastramento de senhas seguras;
- 4) restrição do tempo de conexão dos usuários, quando apropriado;
- 5) procedimentos de entrada e saída no sistema (*logon/logoff*);
- 6) desconexão de terminal por inatividade;
- 7) controle do acesso dos usuários à informação e às funções dos sistemas de aplicação, de acordo com as normas definidas pela OM;
- 8) proteção contra acesso não autorizado para qualquer *software* que seja capaz de sobrepor-se aos controles das aplicações ou do sistema;
- 9) o não comprometimento da segurança de outros sistemas com os quais os recursos de informação são compartilhados; e
- 10) acesso à informação apenas ao seu proprietário, a outros indivíduos nominalmente autorizados ou a determinados grupos de usuários.

i) O monitoramento do uso e acesso ao sistema, com o objetivo de descobrir atividades não autorizadas, fornecendo evidências nos casos de incidentes de segurança, deve ser implementado. Para isso, um registro (*log*) de eventos, com trilhas de auditoria registrando as exceções e outros aspectos de segurança relevantes, deve ser produzido e mantido por um período de tempo acordado para auxiliar em investigações futuras e no monitoramento do controle de acesso.

j) No mínimo, os registros (*log*) de auditoria incluem:

- 1) identificação dos usuários;
- 2) datas e horários de entrada (*logon*) e saída (*logoff*) no sistema;
- 3) identidade do terminal e, quando possível, a sua localização;
- 4) registros das tentativas de acesso ao sistema aceitas e rejeitadas; e
- 5) registros das tentativas de acesso a outros recursos e dados aceitas e rejeitadas.

k) Atenção especial deve ser dada à segurança dos registros de auditoria (*log*) porque, se adulterados, podem gerar uma falsa sensação de segurança.

l) Devem ser implementados controles que impeçam modificações não autorizadas e problemas operacionais, destacando-se:

- 1) desativação dos registros (*log*);

- 2) alterações dos tipos de mensagens que são gravadas;
 - 3) arquivos de registros (*logs*) sendo editados ou excluídos; e
 - 4) esgotamento do meio magnético do arquivo de registros (*logs*), falhas no registro de eventos ou sobreposição do próprio arquivo.
- m) Sistemas disponíveis publicamente.
- 1) É necessário proteger a integridade da informação divulgada eletronicamente, de forma a prevenir modificações não autorizadas que possam afetar a imagem do Exército.
 - 2) A divulgação de informações em sistemas de acesso público, como as existentes em um servidor acessível por meio da internet, necessita estar em conformidade com a legislação vigente.
 - 3) Deve existir um processo de autorização formal, antes da publicação de uma informação.
 - 4) É necessário que os arquivos de programas, dados e outras informações que requeiram alto nível de integridade, expostos em um sistema público, sejam protegidos por um método criptográfico que permita identificar se o arquivo sofreu algum tipo de alteração.
 - 5) Sistemas de publicação eletrônica, especialmente aqueles que permitam retorno (*feedback*) e entrada direta de informações, são cuidadosamente controlados, de forma que:
 - a informação seja obtida em conformidade com a legislação relacionada à proteção de dados;
 - a entrada e o processamento de dados sejam feitos de forma completa e no devido tempo;
 - as informações sensíveis sejam protegidas, durante o processo de coleta e quando armazenadas; e
 - a forma de acesso a sistemas que divulguem informações não permita o acesso casual às redes nas quais esses sistemas estejam conectados.
 - 6) Cuidados no uso da senha:
 - evitar anotação em papéis, agendas e lembretes;
 - não salvar no computador (opção "lembrar senha");
 - mudar periodicamente;
 - não escolher senhas óbvias;
 - não utilizar palavras contidas no dicionário de qualquer língua;
 - não repetir senhas já utilizadas;
 - evitar que novas senhas tenham trechos da anterior;
 - utilizar senhas que possam ser memorizadas e não anotadas;
 - usar senhas diferentes para máquinas diferentes;
 - tomar cuidado com ataques da engenharia social;
 - não emprestar senhas para outros usuários;
 - não utilizar senhas que possam ser facilmente ligadas ao usuário;
 - não informar a senha por e-mail ou por ligação telefônica;
 - não permitir que outrem observe quando a senha estiver sendo digitada;
 - utilizar senha forte com no mínimo 12 (doze) caracteres (algarismos, minúsculas, maiúsculas e caracteres especiais);
 - evitar utilizar, como senha, informações pessoais, nomes próprios ou

combinações sequenciais do teclado (exemplo: asdfg); e

- certificar-se de que:

- cada usuário tenha uma conta individual com senha particular;
- os sistemas em uso só habilitem o acesso mediante o uso de senha forte;
- o arquivo de senhas só possa estar disponível para o administrador; e
- haja troca de senhas forçada pelos sistemas, em intervalos regulares.

3.7.6.5.12 Medidas de segurança de conteúdo da informação nos MTIC

a) **Criptografia:**

- 1) é uma técnica utilizada para tornar ininteligível o texto da mensagem, mediante o emprego de cifras e chaves apoiadas em um algoritmo de transformação;
- 2) a qualidade do algoritmo criptográfico e o tamanho das chaves criptográficas a serem utilizadas são avaliados levando-se em conta o nível de proteção necessário;
- 3) quando as normas de criptografia na OM são implementadas, é necessário atentar para as regulamentações e restrições nacionais que possam ter implicações nas técnicas criptográficas utilizadas em diferentes partes do mundo e com o fluxo de informações criptografadas além das fronteiras;
- 4) a criptografia pode ser de chave simétrica, que utiliza uma mesma chave tanto para codificar como para decodificar informações, ou de chave assimétrica - também conhecida como de chave pública - que utiliza duas chaves distintas, sendo uma pública, que pode ser livremente divulgada, e uma privada, que é mantida em segredo pelo seu proprietário;
- 5) o uso de sistemas criptográficos de origem estrangeira deve ser evitado, buscando-se o desenvolvimento e a adoção de tecnologia do Exército, respeitada a necessidade de interoperabilidade com os sistemas adotados no Ministério da Defesa e no âmbito da Administração Pública Federal, quando pertinente; e
- 6) o uso de sistemas criptográficos no âmbito do Exército está condicionado à certificação de conformidade pelo Departamento de Ciência e Tecnologia.

b) **Autenticação de mensagem:**

- 1) é uma técnica utilizada para garantir a integridade de mensagens enviadas, detectando modificações não autorizadas ou corrupção do seu conteúdo.
- 2) diferentemente da criptografia, essa técnica não é projetada para proteger o conteúdo da mensagem de divulgação não autorizada.

c) **Assinatura digital:**

- 1) fornece o meio para proteção da autenticidade, integridade e não repúdio de documentos eletrônicos;
- 2) é aplicada a qualquer forma de documento processado digitalmente;
- 3) implica considerar o tipo e a qualidade do algoritmo usado e o tamanho da chave; e
- 4) impõe que as chaves criptográficas utilizadas sejam diferentes das usadas para criptografia.

d) **Serviços de irretratabilidade** (não repúdio):

- 1) são usados nos casos em que seja necessário resolver disputas sobre ocorrência ou não de um evento ou ação;
- 2) visam a garantir que o autor não negue ter executado a ação como, por exemplo, criar, enviar ou assinar digitalmente um documento; e
- 3) são baseados no uso de criptografia e técnicas de assinatura digital.

e) **Outras técnicas**

- A aplicação conjunta das técnicas que foram expostas, ou o emprego de outras técnicas, pode ser implementada com o objetivo de buscar maior segurança do conteúdo.

3.7.6.5.13 Medidas de segurança de transmissão da informação nos MTIC

a) **Essas medidas** visam a proteger fisicamente os meios de comunicações, a dificultar a interceptação de mensagens e a consequente análise do seu fluxo.

b) **Todo o tipo de serviço corporativo** de redes de comunicações, seja no contexto local ou remoto, deve contemplar:

- 1) processos de gerenciamento capazes de monitorar e registrar os eventos relativos ao funcionamento dos referidos serviços, de forma a permitir que o fiel cumprimento das regras de Segurança da Informação nos MTIC seja verificado, a partir de autorização pelo escalão superior ou por órgão competente, quando for o caso;
- 2) procedimentos de manutenção dos referidos serviços;
- 3) mecanismos de defesa contra ataques aos referidos sistemas;
- 4) procedimentos para aferir a efetividade das ações adotadas, tanto periódicas quanto inopinadas; e
- 5) medidas de contingência em condições de ativação imediata.

c) **Medidas a serem executadas:**

- 1) esteganografia - método usado para tornar a mensagem imperceptível aos sentidos humanos, mediante o emprego de técnicas específicas. A diferença entre esteganografia e criptografia é que, enquanto esta visa a esconder o conteúdo das mensagens, aquela objetiva esconder a sua existência. Se imaginarmos que um ataque bem-sucedido à criptografia consiste em decodificar uma mensagem cifrada, um ataque bem-sucedido à esteganografia consiste em detectar a mensagem escondida;
- 2) escolha dos locais para instalação dos equipamentos - como primeira providência, impõe-se a necessidade de serem escolhidos os locais para instalação dos equipamentos de TIC. Essa medida visa a criar obstáculos às ações de interceptação; em particular, àquelas voltadas para as linhas que configuram o esquema dos meios de telecomunicações (telefones fixos e móveis, cabos de rede e cabos de fibra ótica, entre outros). Os locais escolhidos são avaliados em razão do fluxo de pessoas, que pode impactar no aumento do risco de ações de espionagem e sabotagem;
- 3) escolha do meio de comunicações - o meio de comunicações a ser empregado deve ser selecionado de acordo com a sensibilidade da informação a ser transmitida. A perfeita adequação é obtida pelo justo

equilíbrio entre os princípios da oportunidade e da segurança. Na escolha do meio a ser empregado, é considerado o aspecto da alternância, buscando-se variações constantes, seja dos equipamentos, operadores ou mensageiros;

4) exploração adequada dos meios de comunicações - essa medida, ligada à anterior, tem por objetivo estabelecer não só os procedimentos que permitam o uso correto dos meios, mas também a disciplina na exploração. Deve ser determinado quem pode transmitir o quê, por quais meios e em que momento;

5) utilização do código de chamada - objetiva estabelecer os procedimentos relativos à exploração de um sistema de sinais convencionados, que confirme ao receptor a real origem da chamada (autenticidade). Visa também, em última análise, a dificultar ações hostis de intromissão na rede de comunicações;

6) exploração do tráfego falso - a utilização de falsas mensagens permite iludir ou confundir o interceptador quanto ao volume e à intensidade do fluxo de mensagens transmitidas, ao mesmo tempo em que pode oferecer ao adversário informação adulterada intencionalmente, neutralizando as ações hostis de busca. Requer planejamento detalhado e execução centralizada; e

7) outras medidas - as Medidas de Proteção Eletrônica (MPE) utilizadas pelo Sistema de Guerra Eletrônica, tal como salto de frequência, dissimulação eletrônica manipulativa, espalhamento espectral e transmissão por salvas são, em sua essência, destinadas à Segurança da Informação na transmissão.

3.7.6.5.14 Segurança dos sistemas de automação de documentos

a) Esses sistemas favorecem a rápida disseminação e compartilhamento de informações, utilizando-se de uma combinação de documentos, computadores, computação móvel, comunicação móvel, correio eletrônico, correio de voz, comunicação de voz em geral, multimídia, serviços postais e máquinas de fax.

b) As considerações relacionadas à segurança das OM, que estão envolvidas com esse conjunto de recursos, incluem:

1) uso de rede segregada;

2) exclusão das informações sensíveis, caso o sistema não forneça o nível de proteção apropriado;

3) especificar os militares, prestadores de serviço ou terceiros autorizados a usarem os sistemas, além dos locais a partir dos quais eles possam ser acessados;

4) restrição de facilidades selecionadas a categorias específicas de usuários;

5) identificação da categoria dos usuários, como, por exemplo, listas dos militares da OM ou prestadores de serviço, em benefício de outros usuários;

6) geração e retenção de arquivos cópias de informação mantidos no sistema; e

7) requisitos e acordos de recuperação e contingência.

3.7.6.5.15 Segurança de redes de computadores

- a) As páginas eletrônicas (*home pages*) devem estar de acordo com as Normas para a Elaboração de Páginas Eletrônicas pelas OM do Exército, na Rede Mundial de Computadores, ou outro instrumento legal que venha a substituí-las, e hospedadas nos domínios disponibilizados pelo Exército.
- b) Os computadores que estiverem conectados à internet, ou a outras redes com acesso remoto, não devem conter informação sensível, particularmente os de Inteligência.
- c) Toda rede, conectada à internet ou não, deve possuir ferramentas atualizadas, capazes de:
 - 1) identificar ou dificultar o acesso de pessoas não autorizadas; e
 - 2) rastrear e emitir relatórios sobre os pontos vulneráveis que podem ser utilizados como porta de entrada para a invasão nos sistemas.
- d) A pasta “público” ou similar, normalmente disponível em redes das OM, não deve ser utilizada para armazenamento de arquivo que contenha informação sensível.

3.7.6.5.16 Segurança no correio eletrônico

- a) O uso de correio-eletrônico (e-mail) com contas oficiais e funcionais sob domínio do Exército Brasileiro é exclusivo para tramitação de assuntos profissionais. Essa ferramenta somente pode ser utilizada para o envio de mensagens contendo informação sensível, se for utilizado um sistema criptográfico.
- b) E-mail particular, que não esteja sob domínio do Exército Brasileiro, não deve ser utilizado para assuntos profissionais.
- c) Os e-mails recebidos de procedência desconhecida não devem ser abertos, principalmente os que contenham arquivos anexados.
- d) O envio de mensagens por meio de correios eletrônicos não corporativos pode comprometer a segurança da informação.

3.7.6.5.17 Trabalho remoto

- a) O trabalho remoto utiliza tecnologia de comunicação para permitir que usuários trabalhem de uma localização física fora da sua OM.
- b) É necessário implantar a proteção apropriada do local do trabalho remoto para evitar, por exemplo, o roubo do equipamento e de informações, a divulgação não autorizada de informação, o acesso remoto não autorizado aos sistemas internos da OM ou o uso impróprio desses recursos.
- c) O trabalho remoto é autorizado pelo Comandante e controlado pelo setor de TIC da OM.
- d) São considerados os seguintes aspectos para utilização de trabalho remoto:
 - 1) a segurança física existente no local;
 - 2) a adequação do ambiente para realização do trabalho remoto;
 - 3) os requisitos de segurança nas comunicações; e
 - 4) o risco de acesso não autorizado à informação por outras pessoas que utilizam o local e não tenham necessidade de conhecer.

e) Os controles e providências que são considerados incluem:

- 1) a provisão de equipamento e mobília apropriados às atividades de trabalho remoto;
- 2) a definição do trabalho permitido, as horas de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços cujo acesso será autorizado;
- 3) a provisão de equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro;
- 4) a segurança física;
- 5) as regras e orientações sobre o acesso de familiares e visitantes ao equipamento e à informação;
- 6) a provisão de suporte e manutenção de equipamento e *software*;
- 7) os procedimentos para cópias de segurança e continuidade do serviço;
- 8) auditoria e monitoramento da segurança; e
- 9) revogação de autoridade, direitos de acesso e devolução do equipamento quando as atividades de trabalho remoto não forem mais necessárias.

3.7.6.5.18 Procedimentos de Backup

a) Com o objetivo de se manter a integridade e a disponibilidade dos serviços de comunicação e processamento da informação, é necessário estabelecer procedimentos para a execução das cópias de arquivos e para a disponibilização dos recursos de reserva.

b) Esses procedimentos são discriminados nas medidas de contingência, de forma a viabilizar a restauração de dados e informações com oportunidade, bem como controlar e registrar eventos e falhas.

3.7.6.5.19 Auditorias e Tratamento de Incidentes

a) Medidas recomendadas:

- 1) identificação e registro das modificações significativas;
 - 2) análise de impacto potencial de tais mudanças;
 - 3) procedimento formal de aprovação das mudanças propostas;
 - 4) comunicação dos detalhes das modificações para todas as pessoas com envolvimento relevante; e
 - 5) procedimentos que identifiquem os responsáveis para a suspensão e recuperação de mudanças no caso de insucesso.
- b) É necessário que as responsabilidades e procedimentos de gerenciamento de incidentes sejam definidos para garantir respostas rápidas, efetivas e ordenadas aos incidentes de segurança.
- c) São estabelecidos procedimentos relativos a todos os tipos potenciais de incidentes de segurança, incluindo:
- 1) falhas dos sistemas de informação e inoperância de serviços;
 - 2) negação de serviço;
 - 3) erros resultantes de dados incompletos ou inconsistentes; e
 - 4) violação de grau de sigilo.

3.7.6.5.20 Medidas de Segurança da Informação em mídias sociais e em aplicativos de TI

- a) É proibida a difusão de informações sensíveis por aplicativos de mensagens instantânea, mídias sociais e redes de relacionamento.
- b) Evitar o uso de mídias sociais e de aplicativos desconhecidos que possam conter funções como geolocalização e compartilhamento de informações pessoais.
- c) O uso de mídias sociais, por militares da ativa do Exército Brasileiro, deve estar em consonância com as regras estabelecidas pela Instituição.

3.7.6.5.21 Medidas de Segurança da Informação nos aparelhos de telefonia celular

- a) Aparelhos celulares são repositórios de dados e informações. Documentos de serviço, de qualquer natureza, não devem ser arquivados nesses aparelhos, que podem ser extraviados, furtados ou roubados, causando o comprometimento dos dados neles arquivados.
- b) Especial atenção deve ser dada a conversas arquivadas em aplicativos de comunicação instantânea e similares. Assuntos de serviço não devem ser tratados por intermédio desse tipo de recurso. Se necessário, utilizar os aplicativos oferecidos pelo Exército Brasileiro.

3.7.6.6 Segurança da Informação nas Áreas e Instalações

3.7.6.6.1 A Segurança da Informação, nas Áreas e Instalações, consiste no subgrupo de medidas voltadas para preservar as informações sobre áreas e instalações pertencentes ou de interesse do Exército.

3.7.6.6.2 Atos de espionagem desenvolvidos com o objetivo de obter informações sobre áreas e instalações são ações hostis a serem consideradas nesse subgrupo de medidas.

3.7.6.6.3 Ações hostis contra áreas e instalações podem ser executadas pelo uso de meios cibernéticos, óticos ou eletrônicos, dentre outros. Por conseguinte, impõe-se a avaliação da existência de informações nas áreas e instalações, que possam ser exploradas pelas ameaças, com o objetivo de definir “onde” e “o quê” será protegido.

3.7.6.6.4 Como exemplo de Informações de Áreas e Instalações a serem protegidas, destacam-se as vistas aéreas, plantas, maquetes e fotografias internas, contidas em arquivos digitais ou físicos, que indiquem os locais da OM sob restrição de acesso, tais como: instalações de comando e controle; paiol; reservas de armamento; reservas de material; e salas dos servidores.

3.7.6.6.5 As medidas de camuflagem, simulação e dissimulação são alguns exemplos de medidas de Segurança da Informação nas Áreas e Instalações.

3.7.6.6.6 A fim de diminuir os riscos concernentes à Segurança da Informação nas Áreas e Instalações, uma medida adequada é não permitir a entrada de pessoas portando equipamentos de comunicação, filmagem ou geração de imagens em áreas e instalações que necessitem ser protegidas. Cuidados especiais devem ser tomados diante da miniaturização desses equipamentos.

3.8 ASSESSORIA TÉCNICA DE CONTRAINTELIGÊNCIA

3.8.1 Assessoria pela qual são orientados os trabalhos de Segurança Orgânica da OM, conforme os grupos de medidas, sendo realizada por meio de visitas de orientação regulares ou inopinadas, por iniciativa própria do Escalão Superior ou por solicitação da OM considerada.

3.8.2 A finalidade da Assessoria Técnica de Contrainteligência (ATCI) é contribuir para a Segurança Orgânica da OM. Para tanto, busca atingir os seguintes objetivos:

- a) levantar as possíveis deficiências de Segurança Orgânica;
- b) propor possíveis soluções para eliminar ou minimizar as deficiências levantadas;
- c) propor medidas para a implantação ou o aprimoramento do PDCl; e
- d) sugerir medidas para o desenvolvimento de atitudes favoráveis à Segurança Orgânica.

CAPÍTULO IV

SEGURANÇA ATIVA

4.1 CONCEITO

4.1.1 É o Segmento da Contraineligência que preconiza a adoção de um conjunto de ações de especialistas, de caráter eminentemente preditivo, destinado a detectar, identificar, avaliar, explorar e neutralizar as ameaças, de qualquer natureza, contra o Exército Brasileiro.

4.2 CONCEPÇÃO

4.2.1 O caráter preditivo implica prospectar as ameaças, visando à adoção de medidas preventivas.

4.2.2 A Segurança Ativa atua dentro e fora do espectro de proteção estabelecido pela Segurança Orgânica.

4.2.3 Na condução dos processos da Segurança Ativa, é normal o emprego dos meios operacionais especializados na busca do dado negado, a fim de subsidiar o planejamento e viabilizar o seu caráter preditivo.

4.2.4 As medidas de Segurança Ativa são implementadas por especialistas, conforme os grupos de medidas, mediante criterioso processo que caracterize um ciclo contínuo de planejamento, execução, controle e realimentação.

A SEGURANÇA ATIVA MANTÉM SEU FOCO NAS AMEAÇAS.

4.3 COMPOSIÇÃO

4.3.1 A Segurança Ativa é composta pelos seguintes grupos de medidas:

- a) Contraespionagem;
- b) Contraterrorismo;
- c) Contrassabotagem;
- d) Contra-ações Psicológicas; e
- e) Contraineligência Interna.

4.3.2 DESINFORMAÇÃO

4.3.2.1 A Desinformação pode ser conceituada, dependendo da sua natureza, como:

- a) técnica especializada utilizada para iludir ou confundir um centro decisor, por meio da manipulação planejada de informações falsas ou verdadeiras, visando, intencionalmente, a induzi-lo a erro de avaliação; ou
- b) fenômeno decorrente de acentuadas deficiências em exatidão, amplitude e/ou aprofundamento das informações disponíveis aos decisores e ao público em geral. A desinformação leva a uma percepção significativamente equivocada, incompleta ou distorcida da realidade e, por fim, promove decisões e comportamentos inadequados às circunstâncias.

4.3.2.2 Embora não seja um grupo de medidas da Segurança Ativa, a Desinformação, empregada por atores hostis, deve ser tratada como ameaça e precisa ser detectada, identificada, avaliada, explorada e neutralizada com oportunidade.

4.3.2.3 A Desinformação permeia todo o segmento de Segurança Ativa.

**A SEGURANÇA ATIVA BUSCA RESPONDER, EM GERAL, AS
SEGUINTE QUESTÕES:**

O QUÊ? QUEM? QUANDO? COMO? ONDE? COM QUE VALOR?

4.4 CONTRAESPIONAGEM

4.4.1 CONCEITO

4.4.1.1 Grupo de medidas destinadas a detectar, identificar, avaliar, explorar e neutralizar ações de espionagem.

4.4.2 CONSIDERAÇÕES GERAIS

4.4.2.1 A espionagem é uma ação realizada por pessoal, vinculado ou não ao serviço de Inteligência, visando à obtenção de conhecimento, dado sigiloso, documento ou material para beneficiar Estados, grupos de países, organizações, facções, empresas, personalidades ou indivíduos.

4.4.2.2 As ações de espionagem, normalmente, são desenvolvidas para beneficiar estados, grupos de países, organizações, facções, grupos de interesse, empresas ou indivíduos.

4.4.2.3 A espionagem pode ser praticada por integrantes do público externo ou interno.

4.4.2.4 As ações de Contraespionagem caracterizam-se pela:

- a) centralização, a fim de ser evitada a quebra de sigilo ou a dispersão de esforços;
- b) compartimentação, com o objetivo de permitir que cada agente saiba apenas o necessário para o cumprimento de sua missão;
- c) integração sistêmica e contínua, a fim de evitar interrupções prejudiciais a essas ações; e
- d) amplitude, para possibilitar a atuação da Contraespionagem em todo o Exército.

4.4.2.5 São considerados alvos prováveis de espionagem no Exército:

- a) adidos militares brasileiros;
- b) pessoal do Exército (civis ou militares), realizando curso ou em outra atividade de serviço no exterior;
- c) pessoal do Exército envolvido em projetos complexos que implicam desenvolvimento de tecnologia de defesa;
- d) empresas ligadas à área de Defesa; e
- e) militares integrantes do SIEx.

4.4.3 MEDIDAS DE CONTRAESPIONAGEM

4.4.3.1 As medidas de Contraespionagem contrapõem-se ao trabalho deliberado de atores hostis, vinculados ou não aos serviços de Inteligência. Entre elas, destacam-se as seguintes:

- a) produzir conhecimentos de Inteligência sobre serviços de Inteligência de outros países;
- b) produzir conhecimento de Inteligência visando à identificação de atores hostis infiltrados ou cooptados;
- c) controlar militares e civis estrangeiros sem visitas ou outras atividades no Exército;
- d) ligar-se com outras agências de Inteligência (nacionais e estrangeiras);
- e) estabelecer redes de colaboradores;
- f) conscientizar a tropa, visando a impedir o recrutamento de integrantes do público interno por atores hostis; e
- g) conscientizar o pessoal no exercício de funções sensíveis, com potencial para se tornar alvos de espionagem.

4.4.4 CONSCIENTIZAÇÃO

4.4.4.1 As medidas de conscientização relativas à Contraespionagem devem ser consideradas no PDCI.

4.5 CONTRATERRORISMO

4.5.1 CONCEITO

4.5.1.1 Grupo de medidas voltado a contribuir para a detecção, identificação, avaliação e neutralização de atos e ameaças terroristas.

4.5.2 CONSIDERAÇÕES GERAIS

4.5.2.1 Terrorismo é a forma de ação que consiste no emprego da violência física ou psicológica, de forma premeditada, por indivíduos ou grupos, apoiados ou não por estados nacionais, com o intuito de coagir um governo, uma autoridade, um indivíduo, um grupo ou mesmo toda a população a adotar determinado comportamento.

4.5.2.2 O terrorismo tornou-se uma ameaça mundial, não existindo fronteiras políticas ou geográficas que limitem o seu alcance.

4.5.2.3 Independentemente de suas origens, tendências ideológicas e objetivos específicos, o terrorismo é objeto de estudo e de interesse permanente da Atividade de Inteligência.

4.5.2.4 Como as ações do terrorismo doméstico e do terrorismo internacional guardam similitude no que se referem aos objetivos, métodos, alvos e outros aspectos, não há necessidade de tratá-los distintamente.

4.5.2.5 A permanente possibilidade de realização de atos de terrorismo implica a adoção de procedimentos básicos, em todos os níveis, para a sua prevenção e combate.

4.5.2.6 A prevenção e o combate às ações terroristas devem ser conduzidos por elementos especializados, porém, de acordo com a situação, elementos não especializados auxiliam nas ações, garantindo o engajamento de todos os setores da segurança e a colaboração da sociedade, sendo necessária a aplicação de conceitos característicos de uma operação de cooperação e coordenação com agências das esferas federal, estadual e municipal.

4.5.2.7 O sucesso da prevenção e combate ao terrorismo depende da existência de um sistema de Inteligência eficiente e eficaz, bem como da coordenação das ações e do compartilhamento de dados e informações.

4.5.2.8 No Exército Brasileiro, o Comando de Operações Especiais (COPEsp) é o elemento especializado no combate ao terrorismo.

4.5.2.9 A prevenção (antiterrorismo) constitui as ações para a proteção caracterizada pela presença ostensiva ou não, de caráter ativo ou passivo, com

a principal finalidade de dissuadir possíveis ameaças. O combate (contraterrorismo) engloba as medidas ofensivas de caráter repressivo, a fim de dissuadir, antecipar, impedir, ou limitar seus efeitos, e responder às ações terroristas.

4.5.2.10 Destaque-se que o Contraterrorismo abordado neste manual é inerente ao ramo Contrainteligência e visa, como grupo de medidas, a contribuir para as atividades executadas pelos elementos encarregados da prevenção e do combate ao terrorismo, particularmente pela produção de conhecimento e pela proteção dos ativos da Força.

4.5.3 MEDIDAS DE CONTRATERRORISMO

4.5.3.1 As medidas a serem adotadas estão relacionadas com ações específicas de Contraterrorismo e outras vinculadas à Segurança Orgânica, destacando-se as seguintes:

- a) levantamento de possíveis atores hostis (inclusive seus apoios e lideranças), suas capacidades, estrutura organizacional e motivações;
- b) estudo detalhado das táticas, técnicas, procedimentos, armamento e equipamento que possam vir a ser empregados;
- c) acompanhamento de atividades clandestinas;
- d) situação das ameaças, conforme explicitado no Capítulo V - Planejamento de Contrainteligência;
- e) negar dados ou conhecimentos aos atores hostis;
- f) proteção de possíveis alvos; e
- g) produção de conhecimento.

4.5.4 CONSCIENTIZAÇÃO

4.5.4.1 As medidas de conscientização relativas ao Contraterrorismo devem ser consideradas no PDCI.

4.6 CONTRASSABOTAGEM

4.6.1 CONCEITO

4.6.1.1 Grupo de medidas da Segurança Ativa destinado a detectar, identificar, avaliar, explorar e neutralizar atos de sabotagem contra a Instituição, pessoas e seus valores, documentos, materiais, equipamentos e instalações, cuja preservação interessa ao Exército Brasileiro.

4.6.2 CONSIDERAÇÕES GERAIS

4.6.2.1 A sabotagem é caracterizada pela realização de qualquer ação sub-reptícia destinada a perturbar, interferir, causar dano, destruir ou

comprometer o funcionamento normal de diferentes sistemas nos campos político, econômico, científico-tecnológico, psicossocial e militar.

4.6.2.2 Os atos de sabotagem podem variar de simples ações individuais, aparentando acidentes, até atos de grande porte com objetivos estratégicos.

4.6.2.3 A sabotagem pode ser confundida com acidente, em meio ao qual, normalmente, as evidências de sua autoria são destruídas.

4.6.2.4 As técnicas e procedimentos empregados em ações de sabotagem são variados, conforme as circunstâncias e as vulnerabilidades envolvidas.

4.6.2.5 Considerando-se que um ato de sabotagem pode estar orientado contra alvos militares e que a sua detecção é difícil, cabe à Contrainteligência estabelecer medidas que permitam reduzir as vulnerabilidades de possíveis alvos, bem como a identificação e a neutralização desse tipo de ação.

4.6.2.6 Nas devidas proporções, as ações inerentes à Contrassabotagem devem ser consideradas por todos os escalões.

4.6.2.7 Os integrantes das OM devem ser conscientizados para adotar procedimentos, a fim de neutralizar ou reduzir os danos decorrentes da sabotagem.

4.6.3 MEDIDAS DE CONTRASSABOTAGEM

4.6.3.1 As medidas de Contrassabotagem devem ser desenvolvidas permanentemente.

4.6.3.2 A adoção de medidas de Contrassabotagem pode ocorrer:

- a) antes que um ato de sabotagem seja consumado; e
- b) após a execução de um ato de sabotagem.

4.6.3.3 Antes de um ato de sabotagem ser consumado, devem ser tomadas as seguintes medidas, entre outras:

- a) produzir conhecimentos de Inteligência que permitam uma ação preventiva oportuna;
- b) levantar os ativos da organização que possam se tornar alvos;
- c) levantar os atores hostis que possam realizar atos de sabotagem contra os ativos do Exército;
- d) levantar as técnicas, táticas e procedimentos adotados por atores hostis que tenham capacidade para realizar atos de sabotagem contra os ativos do Exército;
- e) avaliar os riscos da ocorrência de atos de sabotagem contra esses ativos;
- f) evitar que pessoal orgânico, com indícios de vulnerabilidade, tenha acesso

a material, instalação, informação ou sistemas vitais da organização;
 g) implementar medidas adicionais de segurança para a proteção dos ativos mais suscetíveis a ações de sabotagem;
 h) treinar os quadros para prevenção de acidentes, prevenção e combate a incêndio, além da adoção de procedimentos em outras situações de emergência;
 i) investigar as ocorrências de acidentes, buscando identificar a eventual intenção de causá-los, e acompanhar os eventuais procedimentos investigatórios;
 j) obter meios e estabelecer procedimentos para o controle de danos;
 k) realizar inspeções sistemáticas para verificar vulnerabilidades na segurança dos ativos mais suscetíveis a ações de sabotagem;
 l) evitar a rotina nos procedimentos de segurança; e
 m) realizar o acompanhamento das ocorrências de furto, roubo ou extravio de produtos controlados pelo Sistema de Fiscalização de Produtos Controlados.

4.6.3.4 Após a execução de um ato de sabotagem, devem ser tomadas as seguintes medidas:

a) desencadear o Plano de Segurança Orgânica (PSO);
 b) isolar o local onde se deu a ocorrência, inclusive controlando o acesso de pessoal, visando a mantê-lo intacto para a investigação;
 c) levantar outros alvos vulneráveis ao tipo de ação de sabotagem cometida, e adotar medidas de proteção;
 d) utilizar pessoal de Contraineligência para acompanhar e assessorar os trabalhos de investigação;
 e) levantar testemunhas e material que possam ser úteis na investigação do ocorrido; e
 f) providenciar apoio técnico especializado para o exame do local da ocorrência, a fim de coletar e preservar evidências físicas e levantar todos os indícios possíveis.

4.6.3.5 A investigação deve ser conduzida visando a responder e aprofundar os questionamentos apresentados na figura a seguir:

PERGUNTA	SIGNIFICADO
O QUÊ?	Definir o que efetivamente foi sabotado e os danos causados.
QUANDO?	Estabelecer e confirmar o momento exato do início da ação de sabotagem e o de sua descoberta.
ONDE?	Determinar o local preciso do alvo atingido.
COMO?	Estabelecer o método empregado na sabotagem, os procedimentos e os meios utilizados.
QUEM?	Relacionar suspeitos e listar pessoas ou organizações a quem a ação possa ter beneficiado.
POR QUÊ?	Estabelecer as motivações possíveis para a sabotagem.

Tab 4-1 Questionamentos para a investigação

4.6.4 CONSCIENTIZAÇÃO

4.6.4.1 As medidas de conscientização relativas à Contrassabotagem devem ser consideradas no PDCI.

4.7 CONTRA-AÇÕES PSICOLÓGICAS

4.7.1 CONCEITO

4.7.1.1 Contra-ações Psicológicas

4.7.1.1.1 Grupo de medidas destinado a detectar, identificar, avaliar, explorar e neutralizar a ação psicológica hostil, em especial a propaganda, que possa causar prejuízos e danos ao Exército Brasileiro.

4.7.2 CONSIDERAÇÕES GERAIS

4.7.2.1 As medidas de Contra-ações Psicológicas têm por objetivo anular os efeitos da ação dos instrumentos de influência psicológica sobre o público interno e sobre os segmentos sociais de seu interesse, identificando ações, planejadas ou não, que possam vir a prejudicar a imagem do Exército ou atingir os valores preservados pela Instituição e os seus integrantes.

4.7.2.2 Para a aplicação desse grupo de medidas, adotam-se os seguintes conceitos:

- a) ação psicológica - atividade destinada a fortalecer o moral de grupos amigos e a influenciar os demais públicos-alvo, gerando emoções, atitudes ou comportamentos favoráveis à consecução de objetivos específicos;
- b) fatores psicológicos - fatores de cunho subjetivo que têm potencial para afetar o comportamento humano;
- c) propaganda - difusão de qualquer informação, ideia, doutrina ou apelo especial, visando a gerar emoções, influenciar atitudes e opiniões ou dirigir o comportamento de indivíduos ou grupos, a fim de beneficiar, direta ou indiretamente, quem a promove; e
- d) contrapropaganda - conjunto de ações implementadas no sentido de prevenir, neutralizar ou minimizar os efeitos da propaganda inimiga, adversa ou oponente sobre o público-alvo.

4.7.2.3 Para se tratar de contrapropaganda há, necessariamente, que se entender o conceito da propaganda, pois, em essência, ambas se valem do mesmo processo, variando apenas a finalidade com que são produzidas.

4.7.2.4 A análise da propaganda hostil e a realização da contrapropaganda são conduzidas de acordo com publicações específicas e por especialistas.

4.7.2.5 Genericamente, anular os efeitos de uma ação psicológica hostil implica a obtenção dos seguintes resultados:

- a) tornar os integrantes do Exército imunes aos objetivos da ação psicológica hostil;
- b) impedir que a mensagem da ação psicológica hostil produza os efeitos desejados por sua origem;
- c) fazer com que a ação psicológica hostil produza efeito “bumerangue”; e
- d) gerar, no público-alvo, comportamento favorável ou de aceitação às teses dos temas defendidos, para anular a ação psicológica hostil.

4.7.2.6 Como último recurso, caso não consigam anular os efeitos, as medidas de Contra-ações Psicológicas devem minimizar os efeitos da ação psicológica hostil por meio de técnicas específicas conduzidas por especialistas.

4.7.2.7 O acompanhamento, a análise da ação psicológica hostil e a avaliação da reação do público-alvo aos temas por ela explorados são de fundamental importância para que a finalidade das medidas de Contra-ações Psicológicas seja alcançada.

4.7.3 MEDIDAS DE CONTRA-AÇÕES PSICOLÓGICAS

4.7.3.1 As medidas de Contra-ações Psicológicas são desenvolvidas permanentemente.

4.7.3.2 Essas medidas servem para identificar a eventual necessidade de a avaliação ser realizada por especialistas e, caso necessário, a exploração e a neutralização da ação psicológica ou propaganda hostil.

4.7.3.3 As medidas a serem adotadas estão relacionadas com ações específicas de Contra-ações Psicológicas e outras vinculadas à Segurança Orgânica, destacando-se a conscientização do público interno.

4.7.3.4 A implementação das medidas de Contra-ações Psicológicas divide-se em duas etapas:

- a) 1ª etapa: detecção, identificação e avaliação sumária.
- b) 2ª etapa: avaliação especializada, exploração e neutralização.

4.7.3.5 A 1ª etapa constitui a fase proativa, que contribui para a prevenção contra a ação psicológica hostil.

4.7.3.6 Nessa etapa, realiza-se o planejamento das ações preventivas a serem executadas, buscando neutralizar a motivação e a capacidade de agir do ator hostil.

4.7.3.7 Na 1ª etapa, a detecção e a identificação atuam dentro e fora do espectro de proteção estabelecido pela Segurança Orgânica, visando a prospectar as ameaças para adoção de medidas preventivas.

4.7.3.8 Ainda na 1ª etapa, a análise sumária da ação psicológica hostil pode ser realizada, inicialmente, pelas OM nos diversos níveis. Para isso, o processo descrito no tópico 4.7.4 é a medida utilizada.

4.7.3.9 A 2ª etapa constitui a fase reativa, na qual as medidas necessárias para minimizar ou neutralizar os efeitos da ação psicológica hostil são executadas.

4.7.3.10 Essas medidas são realizadas por especialistas, podendo ser planejadas e coordenadas pela 3ª Seção do escalão considerado ou pelo próprio Sistema de Operações Psicológicas.

4.7.3.11 Não existe um limite que defina precisamente o fim da 1ª etapa e o início da 2ª.

4.7.4 ANÁLISE SUMÁRIA DA AÇÃO PSICOLÓGICA HOSTIL

4.7.4.1 A análise de ação psicológica é um exame da origem e do conteúdo de uma ação psicológica hostil, do público-alvo a que é dirigida, do veículo utilizado e do efeito alcançado.

4.7.4.2 O processo de análise sumária da propaganda hostil é representado pela sigla “OCAVE”: **O**rigem, **C**onteúdo, **A**udiência-alvo (público-alvo), **V**eículo e **E**feito pretendido ou obtido. Essa sigla representa os aspectos essenciais a conhecer sobre a ação psicológica hostil.

4.7.4.2.1 Origem (Quem?)

a) Implica examinar a estrutura da ação psicológica, identificando as organizações e pessoas envolvidas no patrocínio e na emissão da mensagem.

b) Para responder a pergunta “QUEM?”, deve-se identificar a origem o relacionamento com a fonte e a audiência-alvo, bem como os interesses existentes.

c) Deve-se perguntar que aspectos contribuem para a identificação da origem.

4.7.4.2.2 Conteúdo (Diz o quê?)

a) Significa realizar a mesma análise, quantitativa e qualitativa, de todos os símbolos que compõem a mensagem, verificando-se a frequência destes em determinado período de tempo e a intenção velada da origem.

b) Parte mais importante da análise. Deve-se ter total atenção em todos os detalhes da ação psicológica ou propaganda hostil detectada e identificada.

c) Deve-se descrever em detalhes todos os fatores psicológicos observados, vulnerabilidades exploradas (quais apelações emotivas ou dados foram veiculados), linguagem, texto, imagens, sons, bem como se existe correlação com outras mensagens difundidas.

4.7.4.2.3 Audiência-alvo (Para quem?)

- a) Determina-se a parcela do público-alvo que é visada pela ação psicológica hostil, ou para a qual a mensagem é destinada.
- b) Os trabalhos executados devem permitir a identificação das deficiências exploradas pela ação psicológica hostil, localização do público interno, reações anteriores a ações psicológicas similares, adequabilidade e oportunidade da mensagem.

4.7.4.2.4 Veículo (Como?)

- a) Significa determinar o meio difusor da mensagem, identificando suas características, modo de exploração e razões para a sua identificação.
- b) Deve-se perguntar qual o veículo utilizado pelo ator; quais as características do veículo utilizado; qual a data, hora e local da difusão da mensagem ou da detecção.

4.7.4.2.5 Efeito (Para quê?)

- a) Nesse enfoque, procura-se avaliar a mudança de comportamento obtido no público interno a curto, médio e longo prazo.
- b) Deve-se perguntar qual o comportamento realmente apresentado pelo PA.

4.7.4.3 A tabela, a seguir, orienta a condução do Processo de Análise Sumária da Ação Psicológica Hostil.

Pergunta	Significado	Sigla
Quem?	Origem	O
Diz o quê?	Conteúdo	C
Para quem?	Audiência/Alvo	A
Como?	Veículo	V
Para quê?	Efeito	E

Tab 4-2 Processo de Análise Sumária da Ação Psicológica Hostil

4.7.5 CONTROLE DA AÇÃO PSICOLÓGICA HOSTIL

4.7.5.1 Visa à identificação de possíveis ações que possam prejudicar a imagem institucional do Exército ou atingir os valores, os deveres e a ética militar no Exército.

4.7.5.2 Medidas contra outros instrumentos de influência psicológica, que podem afetar negativamente o Exército, também devem ser consideradas pelo decisor.

4.7.6 CONSCIENTIZAÇÃO

4.7.6.1 As medidas de conscientização Contra-ações Psicológicas devem ser consideradas no PDCI.

4.8 CONTRAINTELIGÊNCIA INTERNA

4.8.1 CONCEITO

4.8.1.1 Grupo de medidas da Segurança Ativa destinado a acompanhar as ações dos integrantes do público interno de modo a detectar, identificar, avaliar, explorar e neutralizar ameaças que possam gerar riscos para os valores, os deveres e a ética militar no Exército.

4.8.2 CONSIDERAÇÕES GERAIS

4.8.2.1 As Forças Armadas possuem referenciais fixos, fundamentos imutáveis e universais: os valores militares. São eles que influenciam, de forma consciente ou inconsciente, o comportamento e, em particular, a conduta pessoal de cada integrante da Instituição.



Fig 4-1 Valores Militares

4.8.2.2 Os deveres militares emanam de um conjunto de vínculos morais e jurídicos que ligam o militar à Pátria e à Instituição. Dentre esses deveres, destacam-se a hierarquia e a disciplina, base constitucional das Forças Armadas.

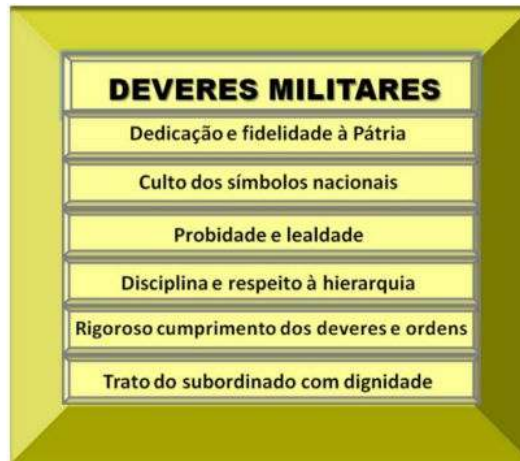


Fig 4-2 Deveres Militares

4.8.2.3 A ética militar é o conjunto de regras ou padrões que levam o militar a agir de acordo com o sentimento do dever, com a honra pessoal, com o pundonor militar e com o decoro da classe. Ela impõe, a cada militar, conduta moral irrepreensível.



Fig 4-3 Ética Militar

4.8.2.4 O culto aos valores, deveres e ética militares impõe que a Instituição disponha de meios para se contrapor às ameaças que possam intimidá-los. A Contraineligência Interna e a ação de comando sintetizam os mecanismos adequados para essa contraposição.

A eficiência, a eficácia e, até mesmo, a sobrevivência do Exército Brasileiro decorrem de um fervoroso culto aos valores, aos deveres e à ética militar.

4.8.3 MEDIDAS DE CONTRAINTELIGÊNCIA INTERNA

4.8.3.1 As medidas de Contrainteligência Interna consubstanciam-se na produção dos seguintes conhecimentos de Inteligência:

- a) infiltração de pessoas ligadas à organização criminosa (ORCRIM);
- b) cooptação de integrantes do público interno por ORCRIM;
- c) envolvimento de integrantes do público interno em vazamentos de dados e conhecimentos ou sensíveis; e
- d) envolvimento de integrantes do público interno com atores hostis, em outras ações que afetem os valores, os deveres e a ética militares.

4.8.4 CONSCIENTIZAÇÃO

4.8.4.1 As medidas de Contrainteligência Interna devem ser consideradas na elaboração do PDCI.

CAPÍTULO V

PLANEJAMENTO DE CONTRAINTELIGÊNCIA

5.1 CONSIDERAÇÕES GERAIS

5.1.1 Este capítulo tem por finalidade orientar o planejamento e a execução das ações relacionadas à Contrainteligência no âmbito do Exército Brasileiro, complementando o planejamento apresentado no Manual de Campanha Planejamento e Emprego da Inteligência Militar.

5.2 CONCEPÇÃO DO PLANEJAMENTO

5.2.1 A concepção do Planejamento de Contrainteligência considera que cada integrante do Exército tem responsabilidades para com as atividades e tarefas de proteção da Força, adotando medidas adequadas às necessidades de sua OM ou de sua respectiva área de responsabilidade. Essas responsabilidades envolvem comportamentos, atitudes preventivas, proatividade e adoção consciente de medidas de segurança efetivas.

5.2.2 A implementação de medidas, sem a análise de todos os aspectos envolvidos, pode causar falhas de segurança, decorrentes de sua insuficiência ou inadequação.

5.2.3 Esse planejamento, responsabilidade do Comandante, é aplicável a todas as OM.

5.2.4 É desejável que esse planejamento seja elaborado por um grupo, sob a supervisão do Oficial de Inteligência.

5.2.5 Em operações, a atuação da Contrainteligência alcança seu nível mais elevado de desenvolvimento e, para cada situação, surge a necessidade da aplicação de medidas específicas, que podem completar ou substituir as existentes. Por conseguinte, no que couber, o planejamento de Contrainteligência relacionado às operações deve seguir o prescrito no Manual de Campanha Planejamento e Emprego da Inteligência Militar.

5.2.6 O planejamento da Segurança Ativa deve ser elaborado por especialistas em cada um dos grupos de medidas desse segmento.

5.3 CONDICIONANTES DO PLANEJAMENTO

5.3.1 O Planejamento de Contraineligência se destina a assegurar o equilíbrio entre a segurança e o funcionamento eficaz, eficiente e efetivo da OM, observando-se as seguintes condicionantes:

- a) ser flexível, simples e factível;
- b) evitar medidas de segurança excessivas ou desnecessárias;
- c) estabelecer coordenação com outras OM nos aspectos que lhes forem comuns ou complementares; e
- d) atender às peculiaridades da OM.

5.4 FASES DO PLANEJAMENTO

5.4.1 As fases do Planejamento de Contraineligência são as seguintes:

- a) Exame de Situação; e
- b) PDCI.

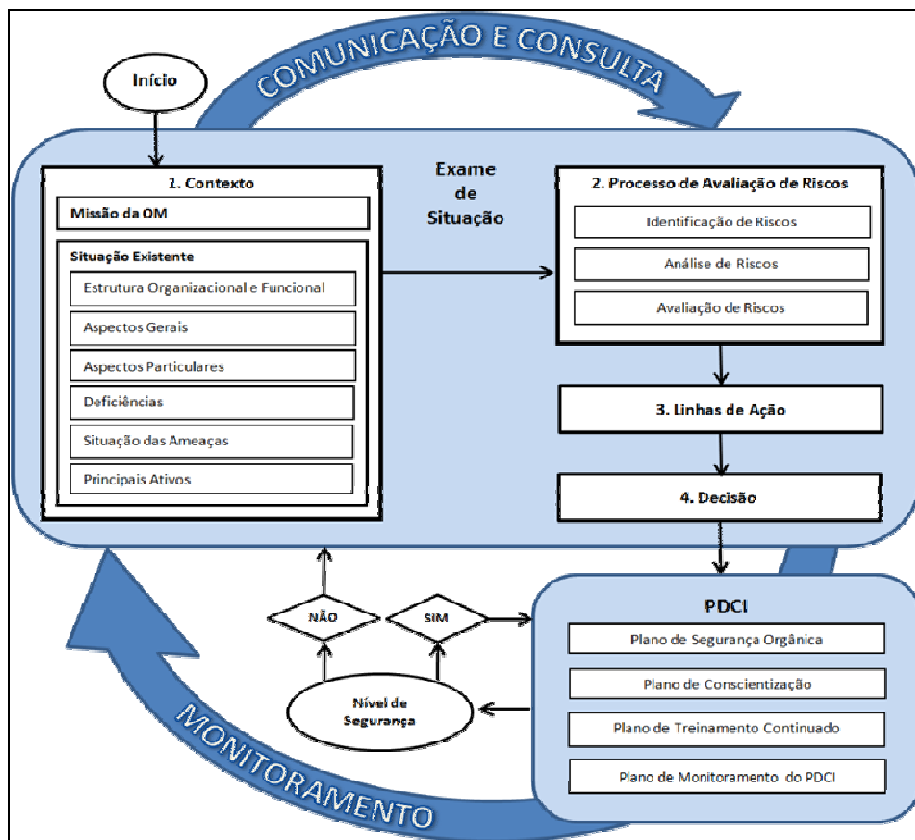


Fig 5-1 Fluxograma do Planejamento

5.4.2 Embora não sejam fases do planejamento, as seguintes atividades devem ser consideradas:

- a) Comunicação e Consulta; e
- b) Monitoramento.

5.4.2.1 A Comunicação e a Consulta são processos contínuos e interativos empregados para tratar com as partes interessadas e obter dados para o planejamento.

5.4.2.2 O Monitoramento é o acompanhamento constante das ações decorrentes do planejamento, possibilitando verificar se o desempenho está de acordo com o esperado e o planejado.

5.5 EXAME DE SITUAÇÃO

5.5.1 FINALIDADE

5.5.1.1 Examinar os diversos fatores atinentes à Contrainteligência, de modo a subsidiar o PDCl.

5.5.2 GENERALIDADES

5.5.2.1 O Exame de Situação (Anexo A) é um processo sistemático de planejamento detalhado que visa a dar uma sequência lógica e ordenada aos diversos fatores que envolvem o processo decisório relacionado à Contrainteligência.

5.5.2.2 O Exame de Situação é detalhado, de acordo com o escalão ao qual se referir.

5.5.2.3 Modificações dos aspectos que integram os fatores da decisão podem ocasionar um novo Exame de Situação e, em consequência, alterações no planejamento.

5.5.3 ETAPAS DO EXAME DE SITUAÇÃO

5.5.3.1 Consideradas as especificidades deste Manual, as etapas do Exame de Situação são as seguintes:

- a) Contexto;
- b) Processo de Avaliação de Riscos;
- c) Linhas de Ação; e
- d) Decisão.

5.5.4 CONTEXTO

5.5.4.1 O contexto estabelece os parâmetros dos ambientes interno e externo que podem impactar a segurança da OM, devendo ser considerados no planejamento.

5.5.4.2 O contexto é composto pela missão da OM e pela situação existente.

5.5.4.3 Missão da OM

5.5.4.3.1 Neste item, deve ser descrita a missão da OM.

5.5.4.4 Situação Existente

5.5.4.4.1 Devem ser considerados os seguintes fatores:

- a) estrutura organizacional e funcional da OM;
- b) aspectos gerais;
- c) aspectos particulares;
- d) deficiências;
- e) situação das ameaças; e
- f) principais ativos da OM.

5.5.4.4.2 Estrutura organizacional e funcional - Neste item, é descrita a organização da OM, subordinação, efetivos, frações constituídas e outras particularidades.

5.5.4.4.3 Aspectos Gerais - Serão observados os seguintes aspectos relativos à OM:

- a) localização;
- b) histórico;
- c) acontecimentos recentes de relevância;
- d) missões específicas atuais; e
- e) orientações do Escalão Superior relacionadas à Contraineligência.

5.5.4.4.4 Aspectos Particulares

a) **Condições meteorológicas:**

1) Condições que possam interferir na Contraineligência da OM, como:

- condições atmosféricas (temperatura, precipitações e nevoeiros);
- ventos (intensidade e direção); e
- histórico de eventos naturais (inundações, secas etc.).

2) Efeitos sobre a Contraineligência na OM, tais como:

- transitabilidade;
- visibilidade;
- pessoal;
- material; e
- áreas e instalações.

b) Terreno:

1) O objetivo do estudo do terreno (ambiente) é determinar os seus aspectos que impactam a Contrainteligência.

2) As informações disponíveis são usadas para efeitos comparativos, mas não são determinantes e suficientes para adoção de medidas de segurança, o que reforça a necessidade do reconhecimento.

3) Além das cartas topográficas, plantas e croquis, os seguintes documentos podem ser úteis:

- Exame de Situação de Inteligência, Anexo de Inteligência e outros documentos pertinentes;
- estudo técnico do terreno;
- relatório de reconhecimento;
- plantas baixas;
- imagens de satélite;
- fotografias aéreas recentes;
- fotografias antigas ou registros da ocorrência de casos que afetaram a Contrainteligência; e
- modelo digital do terreno.

4) Descrição geral da região - os aspectos descritos a seguir são considerados sob o ponto de vista de sua influência para a concretização de ameaças, como acidentes, ACIM, subtração de Material de Emprego Militar (MEM) etc.:

- relevo - conformação do terreno, elevações, depressões, bem como a sua declividade;
- vegetação;
- natureza do solo; e
- hidrografia.

5) Áreas e instalações:

- localização;
- capacitação desses locais;
- deficiências do perímetro;
- controle de veículos no interior da OM;
- iluminação;
- controle de acesso;
- sistemas de alarme;
- sistemas de monitoramento e de registro;
- capacitação das equipes de segurança;
- controle de empregados civis e visitantes; e
- influência de núcleos urbanos no entorno.

6) Aspectos militares:

- observação e campos de tiro;
- cobertas e abrigos;
- obstáculos;
- acidentes capitais; e
- vias de acesso (VA).

c) Recursos disponíveis:

1) Levantar os recursos disponíveis (humanos, materiais e financeiros) de

interesse para a Contraineligência; e

2) Levantar possíveis reforços de outras OM próximas ou com áreas contíguas.

d) Outras considerações:

- Expressão Militar;
- Expressão Política;
- Expressão Econômica;
- Expressão Científico-Tecnológica;
- Expressão Psicossocial; e
- Considerações Cíveis.

5.5.4.4.5 Deficiências

a) o levantamento das deficiências potenciais e existentes pode ser feito por meio da consolidação dos aspectos já estudados no Exame de Situação. Esse levantamento pode, ainda, ser realizado por intermédio de questionamentos ao público interno, utilizando-se de listas de verificação (*checklist*) e pesquisas;

b) a lista de verificação é confeccionada com base em um histórico de deficiências levantadas, devendo ser continuamente atualizada;

c) é necessário definir o que efetivamente precisa ser protegido (ativos), assim como adotar uma postura crítica acerca das deficiências levantadas, de forma que elas possibilitem a identificação das vulnerabilidades da OM diante de ameaças;

d) as vulnerabilidades encontradas devem ser reunidas por grupos de medidas de Segurança Orgânica; e

e) as pesquisas ou listas de verificação devem ser feitas evitando a divulgação das vulnerabilidades da OM.

5.5.4.4.6 Situação das Ameaças

a) Considerando os públicos interno e externo, identificar os atores que tenham capacidade para realizar ações hostis contra os ativos da OM.

b) Para cada ator identificado, levantar as suas possibilidades (ações hostis) e as respectivas motivações que podem levar à realização dessas ações, conforme o modelo sugerido a seguir para fins didáticos:

AMEAÇAS			
ATORES		POSSIBILIDADES (AÇÕES HOSTIS) (2)	MOTIVAÇÕES (3)
UNIVERSO	IDENTIFICAÇÃO (1)		
Público Interno	Ator Alfa	Ação Echo	Motivação 1 Motivação 2
	Ator Bravo	Ação Golf	Motivação 2 Motivação 3
Público Externo	Ator Charlie	Ação Echo	Motivação 1
	Ator Delta	Ação Foxtrot	Motivação 3 Motivação 4
(4)			

Tab 5-1 Situação das Ameaças

Observações:

- (1) Relacionar todos os atores, segundo os públicos interno e externo.
 - (2) Relacionar as ações dos atores que possam afetar negativamente os ativos da OM. Cada ator pode executar uma ou mais ações hostis. Considerar, inclusive, as ações inerentes aos grupos de medidas da Segurança Ativa.
 - (3) Relacionar as motivações do ator para realizar cada ação hostil.
 - (4) Também devem ser identificadas as ameaças decorrentes de fenômenos naturais, condições técnicas, ambientais, materiais ou de outra natureza, que possam originar incidentes de segurança.
- c) A tabela 5-1 é um meio didático para facilitar o entendimento do levantamento das ameaças. Em atendimento ao princípio da simplicidade, é possível que esse levantamento seja feito diretamente por meio do Quadro de Avaliação de Riscos (Tab 5-7).

5.5.4.4.7 Principais Ativos

- a) Identificar os principais ativos por grupo e subgrupo de medidas, conforme o exemplo da tabela, sugerido a seguir para fins didáticos:

GRUPOS DE MEDIDAS	SUBGRUPOS	ATIVOS
Segurança dos Recursos Humanos	-	- Comandante OM - Pessoal em funções sensíveis - Outros integrantes do público interno
Segurança da Informação	a) No pessoal	- Informação sensível
	b) Na documentação	
	c) No material	
	d) Nos meios de TI	
	e) Nas áreas e instalações	
Segurança do Material	-	- Viaturas - Armamento - Munição - Explosivos - Coletes balísticos - Meios de TIC - Outros

Segurança das Áreas e Instalações	-	- Reservas de Armamento - Corpo da Guarda - Paíóis - Instalações de TIC - Arquivo da OM - Almoarifado - Aprovisionamento - PC Comandante - Seções do EM - Seção de Fiscalização Administrativa - Depósitos de outros MEM - Postos de Abastecimento, Lavagem e Lubrificação - Outras
-----------------------------------	---	---

Tab 5-2 Exemplos de ativos, por grupos de medidas

b) O estudo da situação das ameaças e o levantamento dos principais ativos da OM são subsídios para a identificação dos riscos.

5.5.5 PROCESSO DE AVALIAÇÃO DE RISCOS

5.5.5.1 Generalidades

5.5.5.1.1 É o processo global de identificação, análise e avaliação de riscos, que tem por finalidade apresentar os riscos para a organização considerada, criando condições para o seu tratamento.

5.5.5.1.2 Após a realização do Processo de Avaliação de Riscos, o Comandante emite a sua Diretriz para o PDCI (tratamento de riscos).

5.5.5.2 Identificação de Riscos

5.5.5.2.1 Nesta etapa, são identificados os riscos a que a OM está sujeita.

5.5.5.2.2 A identificação inclui todos os riscos, considerando-se os ambientes interno e externo.

5.5.5.2.3 O Exame de Situação é essencial para o levantamento dos dados necessários para a identificação dos riscos.

5.5.5.2.4 Especialistas podem participar, como colaboradores, do processo de identificação dos riscos.

5.5.5.2.5 Para a identificação de riscos, é utilizada uma lista de verificação (*checklist*) e/ou a técnica do *Brainstorming*, de acordo com as peculiaridades

da OM, considerando-se o estudo da situação das ameaças e o levantamento dos principais ativos da OM.

5.5.5.2.6 A identificação dos riscos é realizada, conforme o Quadro de Avaliação de Riscos (Tab 5-7), pelo preenchimento das seguintes colunas: código do risco, ator, ação, motivações e deficiências.

5.5.5.3 Análise de Riscos

a) A análise de riscos tem por fim estabelecer a probabilidade de o risco ocorrer, bem como os seus impactos nos ativos da OM.

b) Os riscos são analisados de maneira qualitativa (subjetiva). Para isso, são utilizados critérios preestabelecidos, com uma escala para determinar o valor de cada risco. A metodologia a ser utilizada possui dois parâmetros claros a serem considerados: probabilidade e impacto.

c) A tabela 5-3 (Avaliação de Probabilidade) apresenta exemplos de descrições e de critérios a serem considerados para o estabelecimento da **probabilidade** de cada risco. Para tanto, são priorizados os critérios julgados preponderantes, de acordo com as especificidades da OM, a qual pode criar outros critérios, conforme a situação específica.

PROBABILIDADE		DESCRIÇÃO E CRITÉRIOS
NÍVEL	VALOR	
MUITO BAIXA	1	a. Descrição - Evento extraordinário para os padrões conhecidos. Não há histórico disponível sobre a sua ocorrência na OM. b. Critérios - Série histórica (probabilidade de ocorrência < 15%). - Motivação do ator (desmotivado). - Capacidade do ator (ator com capacidade mínima). - Fragilidades/deficiências (meios de segurança empregados não apresentam fragilidades/deficiências). - Ambiente fisiográfico, político, econômico, psicossocial e militar (A Op extremamente favorável para o emprego da tropa ou extremamente desfavorável às ameaças).

PROBABILIDADE		DESCRIÇÃO E CRITÉRIOS
NÍVEL	VALOR	
B A I X A	2	a. Descrição - Evento casual, inesperado. Muito embora seja raro, há histórico de sua ocorrência na OM. b. Critérios - Série histórica (15% ≤ probabilidade de ocorrência < 40%). - Motivação do ator (ator com pouca motivação). - Capacidade do ator (ator com pouca capacidade). - Fragilidades/deficiências (meios de segurança empregados, com poucas/inexpressivas fragilidades/deficiências). - Ambiente fisiográfico, político, econômico, psicossocial e militar (A Op favorável para o emprego da tropa ou desfavorável às ameaças).
M É D I A	3	a. Descrição - Evento esperado. Ocorre com frequência reduzida, porém constante. Seu histórico de ocorrência é de conhecimento da OM. b. Critérios - Série histórica (40% ≤ probabilidade de ocorrência < 60%). - Motivação do ator (ator com mediana motivação). - Capacidade do ator (ator com mediana capacidade). - Fragilidades/deficiências (meios de segurança empregados, com medianas fragilidades/deficiências). - Ambiente fisiográfico, político, econômico, psicossocial e militar (A Op medianamente desfavorável para o emprego da tropa ou favorável às ameaças).
A L T A	4	a. Descrição - Evento usual, corriqueiro. Seu histórico é amplamente conhecido pela OM. b. Critérios - Série histórica (60% ≤ probabilidade de ocorrência < 85%). - Motivação do ator (ator motivado). - Capacidade do ator (ator com capacidade). - Fragilidades/deficiências (meios de segurança empregados, com expressivas fragilidades/deficiências). - Ambiente fisiográfico, político, econômico, psicossocial e militar (A Op desfavorável para o emprego da tropa ou favorável às ameaças).

PROBABILIDADE		DESCRIÇÃO E CRITÉRIOS
NÍVEL	VALOR	
MUITO ALTA	5	a. Descrição - Evento se reproduz muitas vezes, frequentemente. Interfere de modo claro nas atividades da OM. b. Critérios - Série histórica (probabilidade de ocorrência $\geq 85\%$). - Motivação do ator (ator com elevada motivação). - Capacidade do ator (ator com elevada capacidade). - Fragilidades/deficiências (meios de segurança empregados, com fragilidades/deficiências extremas). - Ambiente fisiográfico, político, econômico, psicossocial e militar (A Op extremamente desfavorável para o emprego da tropa ou extremamente favorável às ameaças).

Tab 5-3 Avaliação de Probabilidade (modelo)

d) A tabela 5-4 (Avaliação de Impacto) apresenta exemplos de descrições e de critérios a serem considerados para o estabelecimento do **impacto** de cada risco. Para tanto, são priorizados os critérios julgados preponderantes, de acordo com as especificidades da OM, a qual pode criar outros critérios, conforme a situação específica.

IMPACTO		DESCRIÇÃO E CRITÉRIOS (CONSEQUÊNCIAS)
NÍVEL	VALOR	
MUITO BAIXO	1	a. Descrição - Impactos insignificantes nos ativos da OM. b. Critérios - Pessoal (danos insignificantes no público interno). - Imagem do Exército (não afeta, ou afeta minimamente, no âmbito local). - Operacionalidade (não afeta a capacidade/poder de combate para o cumprimento da missão). - Material (não gera danos em material ou instalações da Força). - Financeiro (não gera danos financeiros). - Judicial (não gera processo judicial, mas pode gerar processo administrativo). - Danos colaterais (não gera danos a terceiros ou ao meio ambiente).

BAIXO	2	a. Descrição - Impactos pequenos nos ativos da OM. b. Critérios - Pessoal (danos secundários no público interno). - Imagem do Exército (afeta negativamente, com repercussão local). - Operacionalidade (pequena redução da capacidade/poder de combate para o cumprimento da missão. A OM mantém a capacidade de cumprir a missão). - Material (destruição ou danos de menor monta em MEM ou instalações da OM). - Financeiro (danos financeiros de pequena monta à OM). - Judicial (processo judicial de pequena expressão ou processo administrativo). - Danos colaterais (ferimentos superficiais em terceiros ou degradação de pequena expressão do meio ambiente).
MÉDIO	3	a. Descrição - Impactos significativos nos ativos da OM, porém recuperáveis. b. Critérios - Pessoal (ferimentos leves ou danos morais no público interno). - Imagem do Exército (afeta negativamente, com repercussão regional). - Operacionalidade (redução da capacidade/poder de combate, podendo dificultar o cumprimento da missão). - Material (destruição ou danos em MEM ou instalações da OM). - Financeiro (danos financeiros à OM). - Judicial (processo judicial apenas contra a Instituição). - Danos colaterais (ferimentos em terceiros ou degradação do meio ambiente).
ALTO	4	a. Descrição - Impactos de reversão muito difícil nos ativos da OM. b. Critérios - Pessoal (ferimentos graves no público interno). - Imagem do Exército (afeta negativamente, com repercussão nacional). - Operacionalidade (redução sensível da capacidade/poder de combate, podendo dificultar sobremaneira o cumprimento da missão). - Material (destruição ou danos graves em MEM ou instalações da OM). - Financeiro (danos financeiros graves à OM). - Judicial (processo judicial contra indivíduos ou Instituição). - Danos colaterais (ferimentos em terceiros ou grave degradação do meio ambiente).

MUITO ALTO	5	a. Descrição - Impactos de difícil reversão nos ativos da OM. b. Critérios - Pessoal (morte ou invalidez permanente no público interno). - Imagem do Exército (afeta negativamente, com repercussão internacional). - Operacionalidade (perda da capacidade/poder de combate para o cumprimento da missão). - Material (destruição ou danos irreparáveis em MEM ou instalações da OM). - Financeiro (danos financeiros irreparáveis à OM). - Judicial (processo judicial contra a Instituição ou com possibilidade de responder individualmente perante a justiça comum/Tribunal do Júri). - Danos colaterais (morte/ferimento grave em terceiros ou degradação irreparável do meio ambiente).
------------	---	---

Tab 5-4 Avaliação de Impacto (modelo)

5.5.5.4 Avaliação de Riscos

5.5.5.4.1 Tem por finalidade auxiliar na tomada de decisão para o tratamento dos riscos.

5.5.5.4.2 O **valor do risco** é estabelecido mediante o emprego da Matriz de Exposição a Riscos (Tab 5-5). Para tanto, multiplica-se a probabilidade pelo impacto.

5.5.5.4.3 A Matriz de Exposição a Riscos demonstra a relação entre probabilidade e impacto. Essas duas dimensões de risco, quando combinadas, resultam em um terceiro elemento de risco denominado **Nível de Risco** (baixo, médio, alto e extremo).

I M P A C T O	5 MUITO ALTO	5	10	15	20	25
	4 ALTO	4	8	12	16	20
	3 MÉDIO	3	6	9	12	15
	2 BAIXO	2	4	6	8	10
	1 MUITO BAIXO	1	2	3	4	5
Níveis de risco: - EXTREMO - ALTO - MÉDIO - BAIXO		1 MUITO BAIXA	2 BAIXA	3 MÉDIA	4 ALTA	5 MUITO ALTA
		PROBABILIDADE				

Tab 5-5 Matriz de Exposição a Riscos

5.5.5.4.4 Os níveis de risco são estabelecidos mediante a combinação das dimensões probabilidade x impacto, da seguinte forma:

- Área Vermelha - riscos extremos, que exigem a implementação imediata das ações de proteção e prevenção. São eventos que devem ser monitorados prioritariamente;
- Área Laranja - riscos altos, que devem gerar respostas rápidas, planejadas e testadas em planos de segurança. São eventos que devem ser constantemente monitorados;
- Área Amarela - riscos médios, que devem ser monitorados de forma rotineira e sistemática; e
- Área Verde - riscos baixos, que representam pequenos danos. Esses riscos podem ser somente gerenciados e administrados.

5.5.5.4.5 Possíveis mudanças na probabilidade ou no impacto podem provocar evoluções nos níveis de risco, ou seja, pode haver migração (transformação) de risco baixo para risco alto ou vice-versa.

5.5.5.4.6 A tabela 5-6 (Pontuação por Classificação de Risco) apresenta a classificação dos níveis de riscos e as providências decorrentes, a fim de orientar seu tratamento futuro:

CLASSIFICAÇÃO (NÍVEL)	ÁREA	PONTUAÇÃO	PROVIDÊNCIAS	PRAZO
EXTREMO	VERMELHA	15 a 25	Ação imediata	Desde já
ALTO	LARANJA	8 a 12	Ação no curto prazo	Até 30 dias
CLASSIFICAÇÃO (NÍVEL)	ÁREA	PONTUAÇÃO	PROVIDÊNCIAS	PRAZO
MÉDIO	AMARELA	3 a 6	Ação no médio prazo	Até 100 dias
BAIXO	VERDE	1 a 2	Risco controlável	Indeterminado

Tab 5-6 Pontuação por Classificação de Risco

5.5.5.4.7 Os riscos são numerados (código do risco), a fim de facilitar o seu monitoramento e controle, inclusive quanto às possíveis mudanças de sua ordem de prioridade.

5.5.5.4.8 Os riscos são levantados com o auxílio da tabela apresentada, a seguir:

GRUPO DE MEDIDAS: SEGURANÇA DOS RECURSOS HUMANOS (1)							
IDENTIFICAÇÃO					ANÁLISE		AVALIAÇÃO
Código do risco (2)	Vulnerabilidades			Deficiências (6)	Probabilidade (7)	Impacto (8)	Risco (9)
	Ameaça						
	Ator (3)	Ação (4)	Motivações (5)				
1							
"n"	(10)						

Tab 5-7 Quadro de Avaliação de Riscos (Modelo)

Observações:

- (1) Elaborar as tabelas de avaliação de riscos separando-as por grupos de medidas da Segurança Orgânica.
- (2) Numerar cada risco.
- (3) Relacionar os atores com capacidade para realizar ações hostis sobre os ativos a serem protegidos, inclusive aqueles que podem gerar acidentes.
- (4) Para cada ator, relacionar as ações que podem afetar os ativos a serem protegidos (uma ação por linha). Neste campo, são consideradas, inclusive, as ações inerentes aos grupos de medidas da Segurança Ativa.
- (5) Relacionar as motivações do ator para realizar cada ação hostil.
- (6) Relacionar as deficiências levantadas, podendo agrupá-las, de acordo com a ameaça considerada.
- (7) Quantificar a probabilidade de ocorrência da ação, conforme a Avaliação de Probabilidade (Tab 5-3).
- (8) Quantificar o impacto, conforme a Avaliação de Impacto (Tab 5-4).
- (9) Quantificar o risco, conforme a Matriz de Exposição a Riscos (Tab 5-5).

(10) Relacionar, ao final da tabela, as ameaças decorrentes de fenômenos naturais, condições técnicas, ambientais, materiais ou de outra natureza, que possam originar incidentes de segurança.

Visando a atender ao princípio da simplicidade, em função do tempo disponível para os trabalhos, bem como das necessidades específicas dos decisores, podem ser produzidos e difundidos apenas o contexto e a Avaliação de Riscos.

5.5.5.4.9 Para a elaboração e difusão da Avaliação de Riscos nas condições abordadas no item anterior, o contexto pode ser constituído por documentos de Inteligência, como a Apreciação, a Informação, a Estimativa, o Relatório Especial de Inteligência e o Relatório de ATCI. Nesse caso, a Avaliação de Riscos será um anexo.

5.5.5.4.10 O contexto também pode ser sintético, sendo inserido na página inicial do Quadro de Avaliação de Riscos (Tab 5-7).

5.5.5.4.11 O Quadro de Avaliação de Riscos pode ser difundido, conforme o item 5.5.5.4.9, organizando-se os riscos em ordem decrescente (riscos extremos, altos, médios, baixos e muito baixos, nessa ordem), independentemente dos grupos de medidas.

5.5.6 LINHAS DE AÇÃO

5.5.6.1 Após a avaliação dos riscos, devem ser elaboradas linhas de ação para o seu tratamento.

5.5.6.2 O tratamento decorre das seguintes possibilidades: Aceitar, Compartilhar, Evitar ou Mitigar, sintetizadas pela sigla ACEM, conforme a tabela a seguir.

POSSIBILIDADES	SIGNIFICADO
Aceitar	Nenhuma medida é adotada para reduzir a probabilidade ou o grau de impacto do risco.
Compartilhar	Redução da probabilidade ou do impacto do risco pela transferência ou pelo compartilhamento de uma porção do risco.
Evitar	Abandono das atividades que geram riscos.
Mitigar	Adoção de medidas visando a reduzir a probabilidade, o impacto dos riscos ou ambos.

Tab 5-8 Possibilidades para o Tratamento de Riscos

5.5.6.3 Preferencialmente, são elaboradas, pelo menos, duas linhas de ação para cada risco.

5.5.6.4 Cada linha de ação deve responder aos quesitos: O que fazer? Quem? Quando? Onde? Por quê? Como? Quanto (custo)?

5.5.6.5 As Linhas de Ação, desde que não prejudiquem o princípio da oportunidade (em função do tempo disponível), devem ser montadas de acordo com a tabela a seguir:

GRUPO DE MEDIDAS SEGURANÇA DOS RECURSOS HUMANOS (1)									
Código do risco: (2)									
Classificação inicial (nível do risco): (3)					Classificação inicial (valor do risco): (4)				
Nr LAç	O quê?	Quem?	Quando?	Onde?	Por quê?	Como?	Quanto?	Vantagens	Desvantagens
1	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(12)
n									

Tab 5-9 Linhas de Ação (modelo)

Observações:

(1) Elaborar as linhas de ação, separando-as por grupos de medidas da Segurança Orgânica.

(2) Inserir o número pelo qual o risco foi identificado.

(3) Inserir o nível (extremo, alto, médio ou baixo), conforme a Matriz de Exposição a Riscos.

(4) Quantificar o risco, conforme a Matriz de Exposição a Riscos.

(5) Definir a resposta ao risco (tratamento).

(6) Definir os responsáveis envolvidos.

(7) Estabelecer o prazo de reação, detalhando claramente a data ou período de realização.

(8) Definir os locais onde as atividades/ações serão desenvolvidas.

(9) Justificar a necessidade da ação.

(10) Estabelecer a forma, método ou processo a ser utilizado para o tratamento do risco.

(11) Estimar as necessidades decorrentes da possível implementação de serviços e mecanismos de segurança, dosando-as com a disponibilidade de recursos.

(12) Levantar as vantagens e desvantagens de cada linha de ação, com base nos fatores de comparação (intenção do Comandante, custo, recursos, área de atuação, urgência, valor do risco etc.).

5.5.7 DECISÃO

5.5.7.1 Visando ao tratamento dos riscos, o Comandante toma a sua decisão, escolhendo a melhor linha de ação para a elaboração e a execução do PDCI.

5.5.7.2 Na decisão, o Comandante determina os riscos que serão evitados, aceitos, mitigados ou compartilhados.

5.5.7.3 Os valores dos riscos aceitos devem ser mantidos atualizados.

5.5.7.4 A decisão é expressa por meio de uma Diretriz para o PDCI, que pode ser verbal e deve abordar os seguintes aspectos:

- a) intenção do Comandante;
- b) composição da(s) equipe(s) para a elaboração do PDCI;
- c) prioridade para o tratamento de riscos (Tab 5-10);
- d) respostas aos riscos;
- e) prazo para a elaboração do PDCI;
- f) exclusões (aspectos que não devem ser abordados);
- g) recursos disponíveis (humanos, financeiros e materiais);
- h) planos existentes; e
- i) Outros aspectos julgados úteis (OAJU).

5.5.7.5 A Diretriz para o PDCI tem como anexo, sempre que possível, a Matriz de Tratamento de Riscos (modelo a seguir).

Ordem de Prioridade	Código do Risco	Valor do Risco	Ação	Prazo	Áreas Envolvidas	Medidas	Custo	Responsável
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)

Tab 5-10 Matriz de Tratamento de Riscos (modelo)

Observações:

- (1) Inserir a prioridade para o tratamento do risco.
- (2) Inserir o número pelo qual o risco foi identificado.
- (3) Inserir o valor do risco, conforme o Quadro de Avaliação de Riscos.
- (4) Estabelecer a forma, método ou processo a ser utilizado para o tratamento do risco.
- (5) Inserir o prazo para execução das ações para o tratamento do risco.
- (6) Definir os locais onde as atividades/ações serão desenvolvidas.
- (7) Inserir as medidas necessárias para a execução da ação principal.
- (8) Estimar as necessidades decorrentes da possível implementação de serviços e mecanismos de segurança, dosando-as com a disponibilidade de recursos.
- (9) Definir os responsáveis envolvidos.

5.6 PROCESSO DE DESENVOLVIMENTO DA CONTRAINTELIGÊNCIA

5.6.1 FINALIDADE

5.6.1.1 Planejar, controlar e otimizar as medidas de segurança para proteger pessoas, informações, materiais, áreas e instalações (ativos do Exército), por meio do estabelecimento e da manutenção de medidas de segurança eficientes e eficazes e pelo desenvolvimento da mentalidade de Contrainteligência.

5.6.2 GENERALIDADES

5.6.2.1 O PDCI é um conjunto de atividades contínuas de Contrainteligência estruturado da seguinte forma:

- a) Plano de Segurança Orgânica;
- b) Plano de Conscientização;
- c) Plano de Treinamento Continuo; e
- d) Plano de Monitoramento do PDCI.

5.6.2.2 É necessário conscientizar os integrantes da OM e realizar o monitoramento constantemente, a fim de identificar e tratar os riscos a que a Organização está ou possa vir a ser submetida.

5.6.2.3 As causas de um incidente de segurança estão normalmente associadas a falhas nos procedimentos (obscuros, pouco práticos ou inexistentes), no treinamento (procedimentos existentes mas não conhecidos, aceitos ou entendidos), na liderança (deficiência na ação de comando) ou no indivíduo, componente mais frágil de qualquer sistema de segurança.

5.6.2.4 No PDCI, são consideradas as especificidades da OM onde será aplicado, o que dita o grau de complexidade dos trabalhos a ele inerentes.

5.6.2.5 Inovações e melhorias, como o emprego de MTCT para otimizar os processos, respeitam as práticas consolidadas e aproveitam as soluções desenvolvidas e testadas.

5.6.2.6 As visitas de orientação técnica dos escalões superiores são instrumentos relevantes para transmissão de orientações acerca do PDCI.

5.6.3 CARACTERÍSTICAS FUNDAMENTAIS DO PDCI

5.6.3.1 Simplicidade: objetivo e de conteúdo claro, a fim de reduzir a possibilidade de serem criadas eventuais resistências e incompreensões.

5.6.3.2 Efetividade: capacidade de manter eficácia (obtenção de um efeito desejado) ao longo do tempo.

5.6.3.3 Continuidade: caráter permanente e cíclico.

5.6.4 PLANO DE SEGURANÇA ORGÂNICA

5.6.4.1 É o plano elaborado pelo Oficial de Segurança Orgânica (OSO), auxiliado pelos oficiais do Estado-Maior da OM, que consubstancia as medidas necessárias à implementação da Segurança Orgânica a serem adotadas pela OM.

5.6.4.2 Cabe ao OSO assessorar o Comandante nos assuntos relativos à Segurança Orgânica da OM, revisar e propor a atualização do PSO, bem como orientar, supervisionar e fiscalizar a execução desse Plano.

5.6.4.3 O PSO é composto pelos seguintes planos:

- a) Plano de Bloqueio;
- b) Plano de Monitoramento de Áreas e Instalações;
- c) Plano de Defesa do Aquartelamento;
- d) Plano de Prevenção e Combate a Incêndio; e
- e) Plano de Controle de Danos.

5.6.4.4 O Plano de Bloqueio tem por finalidade estabelecer medidas de segurança visando, particularmente, à criação de barreiras e controles de acesso às áreas de acesso restrito da OM.

5.6.4.5 O Plano de Monitoramento de Áreas e Instalações tem por finalidade permitir a visualização e o registro para auditoria de imagens das ações ocorridas, particularmente, nas áreas sob restrição de acesso da OM.

5.6.4.6 O Plano de Defesa do Aquartelamento tem por finalidade estabelecer procedimentos de segurança, particularmente, para a defesa de áreas e instalações da OM.

5.6.4.7 O Plano de Prevenção e Combate a Incêndio tem por finalidade estabelecer procedimentos visando a prevenir e combater incêndios em áreas e instalações da OM.

5.6.4.8 O Plano de Controle de Danos tem por finalidade estabelecer procedimentos para verificar, sanar ou mitigar, em caso de dano, o comprometimento dos ativos.

5.6.4.9 Medidas a serem consideradas na elaboração do PSO

5.6.4.9.1 Estabelecimento de controles

- a) Controles são medidas de segurança integrantes dos planos anexos ao PSO, adequadas às necessidades particulares da OM.
- b) Alguns controles não são aplicáveis a situações específicas ou podem não ser exequíveis para algumas OM.
- c) Para o estabelecimento dos controles, deve ser considerada a relação entre os custos de implementação e os riscos e perdas potenciais.
- d) Os valores intangíveis, como os danos à imagem do Exército, também devem ser levados em consideração.

- e) Os controles considerados essenciais para uma OM incluem:
- 1) observações sobre o cumprimento de medidas de proteção de dados e informações, privacidade de informações pessoais e segurança de recursos humanos, material, áreas e instalações;
 - 2) salvaguarda de registros organizacionais (físicos e eletrônicos);
 - 3) conferência diária do armamento (Pronto do Armamento) e de outros materiais;
 - 4) TCMS;
 - 5) Termo de Inventário de Documentos ou Material Controlado;
 - 6) Termo de Transferência de Guarda de Documento ou Material Controlado;
 - 7) definição de responsabilidades sobre cada atividade, material ou suporte da informação;
 - 8) participação em instrução e treinamento de Segurança Orgânica; e
 - 9) relatório dos incidentes de segurança.
- f) Outros controles podem ser adotados, de acordo com as especificidades da OM e a Avaliação de Riscos.
- g) Devem ser definidas as responsabilidades pela proteção dos recursos humanos, material, área, instalação e informação, ou suporte desta, bem como pelo cumprimento de procedimentos de segurança específicos.
- h) No PSO, devem ser atribuídas regras e responsabilidades de Contraineligência, que podem ser complementadas com orientações detalhadas.
- i) Os processos de segurança atinentes a cada atividade devem estar identificados, documentados e com os níveis de autorização e acesso definidos claramente.

5.6.4.9.2 Serviços de Segurança

- a) São os serviços de escala voltados para a Segurança Orgânica da OM, bem como os encargos de Contraineligência inerentes à Seção de Inteligência.
- b) Esses serviços visam a proporcionar a segurança dos recursos humanos, da informação, do material, de área e de instalações, estabelecendo barreiras entre os ativos de uma OM e os atores hostis, sendo caracterizados pelo(a):
- 1) defesa externa do perímetro da OM;
 - 2) controle e registro de entrada e saída de pessoal e material da OM;
 - 3) controle e registro de entrada e saída de pessoal e material das instalações de acesso restrito;
 - 4) defesa ou vigilância de instalações específicas no interior do perímetro (paióis, garagens, posto de combustível, reservas de material bélico etc.); e
 - 5) fiscalização diária e contínua desses serviços.

5.6.4.9.3 Mecanismos de Segurança

- a) São equipamentos mecânicos ou eletrônicos aplicados à segurança, tais como:
- 1) controle de acesso eletrônico na porta de entrada de instalações de acesso restrito;

- 2) alarmes e detectores de intrusão em instalações de acesso restrito que devam ser lacradas ao final do expediente;
 - 3) sistemas de monitoramento eletrônico e de registro; e
 - 4) utilização de dois cadeados na(s) porta(s) de acesso, especialmente nas reservas de armamento, com as respectivas chaves sob a guarda de pessoas distintas.
- b) A seleção de mecanismos de segurança deve ser feita com base nos principais ativos a serem protegidos, tanto no que se refere à TIC quanto aos riscos físicos.
- c) Os mecanismos de segurança são prioritariamente preventivos e visam a evitar a ocorrência de danos aos ativos da OM, com destaque para roubo, invasão em força, incêndio, explosões e interrupções no fornecimento de energia elétrica.
- d) Os aspectos ambientais são monitorados de forma proativa para permitir à OM antecipar-se a condições que possam afetar desfavoravelmente os seus ativos.

5.6.4.9.4 Medidas de Contingência

- a) São estabelecidas com o objetivo de prover meios e procedimentos alternativos, diante de situações que ameacem a segurança, com o intuito de assegurar a continuidade ou restabelecer o funcionamento dos ativos afetados.
- b) Dentre as medidas de contingência que integram os planos que compõem o PSO, podem ser definidos procedimentos adicionais de segurança tais como o estabelecimento de equipes de pronta-resposta, que possibilitam a detecção e avaliação dos riscos em tempo real, permitindo que as providências necessárias sejam tomadas com oportunidade.
- c) A capacidade da OM responder às situações de emergência está diretamente relacionada à realização de treinamentos adequados e direcionados aos procedimentos a serem adotados em cada situação particular.
- d) Deve, também, ser considerado o impacto negativo de um desastre que possa ocorrer nas proximidades de uma instalação como, por exemplo, incêndio em prédio vizinho, bem como o seu alcance (repercussão).
- e) As medidas relativas estritamente à Segurança Ativa são adotadas, conforme planejamento específico de especialistas, em cada um dos grupos de medidas desse segmento.

5.6.4.9.5 Medidas de Controle de Danos

- a) Visam a possibilitar a verificação, a solução ou a mitigação do dano aos ativos que deveriam ter sido protegidos.
- b) É desejável que as medidas de controle de danos estejam alinhadas com as do Escalão Superior.
- c) Quando da ocorrência de dano(s), as seguintes medidas devem ser adotadas imediatamente:
- 1) identificação da área atingida;
 - 2) avaliação da extensão dos danos; e

3) estabelecimento de prioridades quando mais de uma instalação for atingida, para o emprego dos grupos, turmas ou equipes de controle de danos.

d) A atuação dos elementos de controle de danos, normalmente, consiste em:

1) assumir a direção das atividades nas instalações onde os responsáveis tiverem perdido o controle da situação;

2) auxiliar nas medidas necessárias para a rápida normalização dos trabalhos interrompidos;

3) avaliar a extensão real dos danos e as providências necessárias para o seu controle;

4) acionar os seus meios orgânicos e os disponíveis no local, para fazer face às consequências da ação hostil ou catástrofe da natureza;

5) cooperar para o estabelecimento ou funcionamento do sistema de evacuação de feridos, do local até uma instalação de saúde de emergência, se esta houver sido instituída;

6) cooperar na localização, identificação e evacuação de mortos, de acordo com as normas estabelecidas; e

7) restabelecer as condições de funcionamento da instalação, procurando, imediatamente, normalizar a atividade que tiver sido interrompida.

e) Levantamento de danos:

1) consiste em um exame direto do ativo afetado, a fim de estimar os danos causados. Constitui a base para as ações subsequentes de controle de danos;

2) com base nesse levantamento, são determinadas as equipes necessárias para a execução das ações de controle de danos;

3) essas equipes, formadas com elementos, seções, grupos, pelotões ou integrantes de instalações pertencentes à OM afetada, são organizadas de modo funcional, isto é, orientadas para os diversos tipos de incidentes que podem ocorrer no controle de danos; e

4) é importante, para a manutenção da eficiência das equipes, que elas sejam organizadas e empregadas por frações constituídas, isto é, mantendo-se a organização com a qual desempenham suas atividades normais e sendo lideradas pelos respectivos comandantes.

f) As seguintes medidas de controle de danos podem ser executadas:

1) isolar os locais ou áreas atingidas, impedindo a entrada de pessoas não autorizadas e a saída de qualquer pessoa, até segunda ordem;

2) o encarregado de cada setor, seção ou fração deve providenciar o levantamento dos eventuais danos ocorridos, consolidando os dados em relatório a ser encaminhado ao comando da OM. Também deve, na esfera de suas atribuições, adotar as providências necessárias para o restabelecimento do funcionamento do setor, seção ou fração sob sua responsabilidade;

3) em função da gravidade do fato gerador das medidas de contingência, a OM ficará em condições de emitir uma nota de esclarecimento à imprensa, conforme as orientações do Centro de Comunicação Social do Exército (CComSEx);

4) quando for necessária a realização de perícia do Corpo de Bombeiros ou da Polícia, deve ser escalado um oficial de ligação para acompanhar as diligências que ocorrerão;

- 5) nos casos de evacuação médica, deve ser previsto, em função da gravidade do caso, o acompanhamento do paciente por um médico ou enfermeiro, de modo que as condições do atendimento sejam verificadas;
- 6) em caso de falecimento de militar ou servidor civil, a OM deve tomar todas as providências relacionadas aos familiares (desembarço do corpo, documentação e o seu transporte, bem como os cerimoniais compatíveis a cada religião);
- 7) no caso de acesso indevido ou vazamento de informação sensível, as consequências desse fato devem ser precisamente avaliadas, particularmente quanto ao uso do conteúdo da informação face ao risco de desgaste da imagem da Instituição;
- 8) após a volta à normalidade em todos os setores da OM, deve ser realizada uma Análise Pós Ação, para retificar ou ratificar o Plano de Controle de Danos;
- 9) estabelecer comunicação com os afetados ou envolvidos na recuperação de incidentes;
- 10) encaminhar relato da ação à autoridade apropriada; e
- 11) empregar a Comunicação Social, se necessário.

5.6.4.10 O Anexo B apresenta um modelo de PSO.

5.6.5 PLANO DE CONSCIENTIZAÇÃO

5.6.5.1 É um plano que regula as ações que visam a desenvolver e manter atitudes favoráveis ao PDCI pelos integrantes da OM.

5.6.5.2 Baseia-se na execução de ações cognitivas e afetivas que visam a criar ou desenvolver a mentalidade de Contraineligência nos integrantes da OM e sensibilizá-los para adotar comportamentos favoráveis à implantação do PDCI.

5.6.5.3 Apesar do esforço de sensibilização e de comprometimento da OM, essa tarefa continuará sendo objeto de atenção constante.

5.6.5.4 Podem ser utilizados diversos instrumentos de conscientização, tais como vídeos educativos, estudos de caso, *softwares* de simulação, mídia impressa, mensagens de Contraineligência, palestras com especialistas, reuniões sociais, desportivas e culturais.

5.6.5.5 As mensagens de Contraineligência visam a alertar o público-alvo sobre riscos à segurança a serem evitados. Elas podem ser difundidas por escrito, sob a forma de áudios ou vídeos. A figura 5-2 apresenta um exemplo.

A utilização de aplicativos de mensagens instantâneas para difundir dados ou conhecimentos sensíveis cria risco desnecessário para a segurança da informação.

Fig 5-2 Mensagem de Contraineligência

5.6.5.6 A atuação dos oficiais e praças e a compreensão de todos os participantes do processo são fundamentais para o sucesso do PDCI.

5.6.5.7 O Anexo C apresenta um modelo de Plano de Conscientização.

5.6.6 PLANO DE TREINAMENTO CONTINUADO

5.6.6.1 É um plano que regula o desenvolvimento da instrução e dos integrantes da OM, visando à execução das ações previstas no PDCI.

5.6.6.2 Define os assuntos a serem abordados nas instruções para os integrantes da OM, podendo ser modificado a qualquer tempo, em decorrência de falhas ou da necessidade de correções no desenvolvimento da Contraineligência.

5.6.6.3 É importante estabelecer um processo educacional que contenha padrões de comportamento para evitar que a OM se torne potencialmente vulnerável a vazamentos e a outras ações hostis.

5.6.6.4 Devem ser previstos objetivos de Contraineligência nos currículos dos diferentes programas de instrução e nas instruções de quadros das OM.

5.6.6.5 Os programas de instrução da OM devem disponibilizar tempo para as instruções necessárias à implantação do PDCI. Os assuntos a serem ministrados devem ter diferentes abordagens, de acordo com os círculos hierárquicos.

5.6.6.6 Dentre outros assuntos, podem ser ministrados os seguintes: fundamentos de Contraineligência, principalmente no segmento Segurança Orgânica, avaliação de riscos, lições aprendidas, normas e procedimentos da OM e lista de verificação (*checklist*).

5.6.6.7 Os novos integrantes do Exército devem receber instruções com o objetivo de criar, desenvolver e manter a mentalidade de Contraineligência, bem como transmitir os procedimentos preventivos para o trato com informação ou material sensível.

5.6.6.8 Os aspectos necessários à eliminação das causas de incidentes de segurança, a princípio, são objeto de instrução.

5.6.6.9 O processo educativo tem início na admissão e só é finalizado por ocasião do desligamento do militar da Força.

5.6.6.10 Todo militar recém-chegado a uma OM deve receber orientações de Segurança Orgânica, considerando, também, os aspectos específicos da OM.

5.6.6.11 O Plano deve conter três elementos básicos:

- a) orientação inicial, visando a explicar a razão das medidas de Contrainteligência e os motivos para o seu cumprimento;
- b) orientação específica, visando a informar quais são as medidas de Contrainteligência e como proceder para cumpri-las; e
- c) orientação periódica, reforçando a necessidade de acatamento das técnicas e procedimentos relativos à Contrainteligência.

5.6.6.12 O Anexo D apresenta um modelo de Plano de Treinamento Continuado.

5.6.7 PLANO DE MONITORAMENTO DO PDCI

5.6.7.1 É um plano estabelecido com a finalidade de controlar permanentemente os planos que compõem o PDCI, identificando oportunidades de melhoria, bem como a sua realimentação.

5.6.7.2 O monitoramento é realizado por intermédio de inspeções (auditorias) programadas ou inopinadas.

5.6.7.3 Os dados para análise de problemas internos, sob a ótica da Contrainteligência, devem ser coletados e mantidos em segurança.

5.6.7.4 Em função dos dados levantados, pode ser necessário o planejamento de novas ações para a correção de distorções porventura encontradas no PDCI.

5.6.7.5 A validação dos procedimentos de Contrainteligência é alcançada na consecução das metas estabelecidas, dos indicadores de desempenho e dos parâmetros de verificação.

5.6.7.6 O monitoramento do PDCI visa a gerenciar, auditar e validar os planos que o compõem, diferindo do monitoramento do planejamento de Contrainteligência, que, em síntese, tem por fim verificar a efetividade desse planejamento.

5.6.7.7 O Anexo E apresenta um modelo de Plano de Monitoramento do PDCI.

ANEXO A

MEMENTO DO EXAME DE SITUAÇÃO DE CONTRAINTELIGÊNCIA

Organização:

Local:

Data-hora:

1. MISSÃO DA OM

- Descrição da missão da OM

2. SITUAÇÃO EXISTENTE**a. Estrutura Organizacional e Funcional da OM****b. Aspectos Gerais**

- 1) Localização da OM
- 2) Histórico (fatos que tiveram impacto para a OM no contexto regional)
- 3) Acontecimentos recentes de relevância
- 4) Missões específicas atuais
- 5) Orientações do Esc Sp relacionadas à Contrainteligência

c. Aspectos Particulares

- 1) Condições meteorológicas
 - a) Condições existentes que possam interferir na Contrainteligência
 - (1) Condições atmosféricas (temperatura, precipitações e nevoeiros)
 - (2) Ventos (intensidade e direção)
 - (3) Histórico de eventos naturais (inundações, secas etc.)
 - b) Efeitos sobre a Contrainteligência
 - (1) Transitabilidade
 - (2) Visibilidade
 - (3) Pessoal
 - (4) Material
 - (5) Áreas e instalações
- 2) Terreno
 - a) Descrição geral da região (aspectos que impactam a Contrainteligência)
 - (1) Relevo
 - (2) Vegetação
 - (3) Natureza do solo
 - (4) Hidrografia
 - (5) Áreas e Instalações
 - b) Localização
 - b) Identificação das pessoas que têm acesso
 - c) Deficiências do perímetro
 - d) Controle de veículos
 - e) Iluminação
 - f) Controle de acesso

- g) Sistemas de alarme
- h) Sistema de monitoramento e de registro
- i) Capacitação das equipes de segurança
- j) Controle de empregados civis e visitantes
- k) Responsáveis pela segurança
- l) Núcleos urbanos importantes
- 4) Aspectos militares
 - a) Observação e campos de tiro
 - b) Cobertas e abrigos
 - c) Obstáculos
 - d) Acidentes capitais
 - e) Vias de acesso
- 5) Recursos disponíveis
 - a) Humanos
 - b) Materiais
 - c) Financeiros
- 6) Outras considerações
 - a) Expressão Militar
 - (1) Órgãos de Segurança Pública (OSP)
 - (2) Recrutamento e treinamento
 - (3) Coesão interna
 - (4) Ilícitos
 - (5) Traços de personalidade
 - b) Expressão Política
 - c) Expressão Econômica
 - d) Expressão Científico-Tecnológica
 - e) Expressão Psicossocial
 - f) Considerações Civis

d. Deficiências

- 1) Segurança dos Recursos Humanos
- 2) Segurança do Material
- 3) Segurança das Áreas e Instalações
- 4) Segurança da Informação
 - a) No Pessoal
 - b) Na Documentação
 - c) No Material
 - d) Nos Meios de Tecnologia da Informação e Comunicações
 - e) Nas Áreas e Instalações

e. Situação das Ameaças (identificação, composição e possibilidades)

ATORES HOSTIS		POSSIBILIDADES (AÇÕES HOSTIS)	MOTIVAÇÕES
UNIVERSO	IDENTIFICAÇÃO		
Público Interno	Ator X	Ação X	Motivação X
Público Externo	Ator Y	Ação Y	Motivação Y

f. Principais Ativos da OM

GRUPOS DE MEDIDAS	SUBGRUPOS	ATIVOS

3. **PROCESSO DE AVALIAÇÃO DE RISCOS**a. Identificação, Análise e Avaliação de Riscos

GRUPO DE MEDIDAS: SEGURANÇA DOS RECURSOS HUMANOS							
IDENTIFICAÇÃO					ANÁLISE		AVALIAÇÃO
Código do risco	Vulnerabilidades						
	Ameaça			Deficiências			
	Ator	Ação	Motivações				
					Probabilidade	Impacto	Risco

4. **LINHAS DE AÇÃO**

GRUPO DE MEDIDAS:									
Código do risco:									
Classificação inicial (nível do risco):					Classificação inicial (valor do risco):				
Nr LAç	O quê?	Quem?	Quando?	Onde?	Por quê?	Como?	Quando?	Vantagens	Desvantagens

5. **DECISÃO**

- Escolha, pelo Comandante da linha de ação, que atenda, nas melhores condições, o cumprimento da missão.
- O Comandante determinará os riscos que serão evitados, aceitos, mitigados e compartilhados.
- A decisão é expressa por meio da Diretriz para o PDCL.

ANEXO B**PLANO DE SEGURANÇA ORGÂNICA
(MODELO)**

Organização:

Local:

Data:

1. SITUAÇÃO

- Relatar, de forma sucinta e clara, os aspectos abordados no Exame de Situação, assim como as razões que levaram o Comandante da OM a decidir pela adoção das medidas de segurança consubstanciadas neste Plano.

2. MISSÃO

- Salvar os ativos da OM.

3. EXECUÇÃO

a. Segurança dos Recursos Humanos

b. Segurança da Informação (no Pessoal, na Documentação, no Material, nos Meios de TI, nas Áreas e Instalações)

c. Segurança do Material

d. Segurança da Informação nas Áreas e Instalações

4. PRESCRIÇÕES DIVERSAS

- Observações ou ordens específicas não relatadas anteriormente.

Assinatura
COMANDANTE

APÊNDICES

- 1 - PLANO DE BLOQUEIO (Omitido)
- 2 - PLANO DE MONITORAMENTO DE ÁREAS E INSTALAÇÕES (Omitido)
- 3 - PLANO DE DEFESA DO AQUARTELAMENTO (Omitido)
- 4 - PLANO DE PREVENÇÃO E COMBATE A INCÊNDIO (Omitido)
- 5 - PLANO DE CONTROLE DE DANOS (Omitido)
- 6 - SUGESTÕES SOBRE SEGURANÇA ORGÂNICA

APÊNDICE 1 AO ANEXO B**SUGESTÕES SOBRE SEGURANÇA ORGÂNICA**

1. Não deposite na cesta de papéis: rascunhos e cópias contendo dados ou informações sensíveis. Use o triturador e incinere os documentos inservíveis diariamente.
2. Retire de sua mesa de trabalho, antes de deixar a sala, documentos que não devem ficar expostos, guardando-os em local apropriado. Ao término do expediente, verifique se os arquivos, gavetas e portas de armários estão fechados e trancados.
3. Assunto sigiloso não se trata por telefone. Não há segurança neste meio de comunicação.
4. A sua condição ou suas atribuições de serviço não deverão ser objeto de conversas em reuniões sociais, bares, restaurantes, coletivos etc.
5. Tenha em mente que, em reuniões sociais, você não sabe quem está escutando.
6. No serviço, não procure inteirar-se de assuntos que não sejam de suas atribuições ou não estejam sob sua responsabilidade. Respeite a necessidade de conhecer.
7. Informações sobre documentos somente deverão ser fornecidas a quem estiver devidamente credenciado e tiver necessidade de conhecer.
8. Lembre-se de que a necessidade de conhecer dados e informações sigilosas depende da função desempenhada e não do seu grau hierárquico.
9. Qualquer indício de risco para a segurança dos recursos humanos, das informações, do material e das áreas e instalações deve ser imediatamente comunicado ao OSO da sua OM.
10. Colabore com a Guarda do Quartel e o pessoal de serviço. Eles estão ajudando a cumprir as normas de segurança.

ANEXO C**PLANO DE CONSCIENTIZAÇÃO
(MODELO)**

Organização:

Local:

Data-hora:

1. FINALIDADE

- Apresentar um conjunto de medidas voltadas para obter e manter atitudes favoráveis ao Processo de Desenvolvimento da Contraineligência (PDCI) pelos integrantes da OM considerada.

2. OBJETIVOS

- Citar o(s) objetivos(s) a serem alcançados com a implementação do Plano de Conscientização.

3. CONDIÇÕES DE EXECUÇÃO

- Explicar, de maneira sucinta, de que forma a OM pretende desenvolver a conscientização sobre a importância do PDCI na OM.
 - Deverão ser definidos os públicos-alvo que serão objetos das campanhas de conscientização.
 - Deverá ser estabelecido um cronograma para a implementação do Plano de Conscientização, que poderá ser um apêndice ao anexo.
 - Definir o emprego das ferramentas e métodos de conscientização. Por exemplo:

FERRAMENTAS E MÉTODOS DE CONSCIENTIZAÇÃO	PÚBLICO-ALVO		
	ALFA	BRAVO	CHARLIE
Mensagem de Contraineligência			
Palestras de Especialistas			
Quadro Mural			
Folder de Segurança Orgânica			
Semana de Segurança Orgânica			
Vídeo educativo			
Cartilha de Segurança Orgânica			
Cartaz de Contraineligência			

Banner de Contraineligência			
Totem digital			
Vídeo Institucional para Visitantes			
Pesquisa de Opinião sobre Segurança			
Estudos de Caso			
Softwares de Simulação			

- Na sequência, poderá ser explicado o objetivo de cada instrumento, bem como apresentados modelos, definidos locais de exposição e outros aspectos julgados úteis.

4. PRESCRIÇÕES DIVERSAS

- Observações ou ordens específicas não relatadas anteriormente.

Assinatura
COMANDANTE

ANEXO D**PLANO DE TREINAMENTO CONTINUADO**

Organização:

Local:

Data-hora:

1. FINALIDADE

- Regular e normatizar o estabelecimento de ações voltadas para a implementação de medidas de Contraineligência na OM considerada, no que concerne à implantação do Plano de Treinamento Continuoado.

2. OBJETIVOS

- Citar o(s) objetivo(s) a serem alcançados com a implementação do Plano de Treinamento Continuoado.

3. CONDIÇÕES DE EXECUÇÃO

- a. Detalhar as ações planejadas, especificando prazos e responsabilidades.
- b. Definir os assuntos, o público-alvo e os períodos em que se desenvolverão as instruções.
- c. As atividades programadas deverão abordar todos os grupos de medidas da Segurança Orgânica.
- d. Estabelecer indicadores de desempenho e instrumentos de avaliação.
- e. Elaborar um Cronograma de Atividades que contenha três elementos básicos:
 - 1) orientação inicial, visando a explicar a razão das medidas de Contraineligência e os motivos para o seu cumprimento;
 - 2) orientação específica, visando a informar quais são as medidas de Contraineligência e como proceder para cumpri-las; e
 - 3) orientação periódica, reforçando a necessidade de acatamento das técnicas e procedimentos relativos à Contraineligência.

4. PRESCRIÇÕES DIVERSAS

- Detalhamento das coordenações necessárias à implantação do Plano de Treinamento Continuoado.

Assinatura
COMANDANTE

ANEXO E**PLANO DE MONITORAMENTO DO PDCI**

Organização:

Local:

Data-hora:

1. FINALIDADE

- Apresentar um conjunto de medidas voltadas para controlar permanentemente as fases do planejamento, identificando oportunidades de melhoria, bem como realimentando esse Plano.

2. OBJETIVOS

- Citar o(s) objetivo(s) a serem alcançados com a implementação do Plano de Monitoramento. Exemplos: garantir que os controles sejam eficazes e eficientes; obter informações adicionais para melhorar o processo de avaliação de riscos; analisar os eventos, mudanças, tendências, sucessos e fracassos e aprender com eles; detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco; e identificar riscos emergentes.

3. CONDIÇÕES DE EXECUÇÃO**a. Gerência**

- Designar uma Equipe de Gerência.
- Detalhar a estruturação e as atribuições da Comissão de Gerência responsável por coordenar e fiscalizar a execução de todas as ações planejadas.

b. Auditoria

- Estabelecer a Equipe de Auditoria, a qual deverá confeccionar os relatórios das auditorias realizadas e encaminhá-los à Equipe de Validação.
- Detalhar o planejamento das auditorias, podendo ser estas realizadas de forma programada, inopinada ou solicitada.
- Estabelecer um Cronograma de Execução das Auditorias e das Revisões dos Planos. Sugere-se a realização das auditorias e revisões dentro do período de 1 (um) ano.
- As auditorias, ainda que limitadas, deverão ser programadas de forma a contemplar todos os grupos de medidas de Segurança Orgânica.
- As auditorias deverão ter como ponto de partida os relatórios anteriores, visando a verificar as ações corretivas.

c. Validação

- Estabelecer Equipe de Validação, por setor.
- A Equipe de Validação deverá analisar os relatórios das auditorias

realizadas e confeccionar o relatório de validação. É importante que o relatório de validação seja publicado no Boletim de Acesso Restrito da OM.

4. MEDIDAS DE COORDENAÇÃO E CONTROLE

- Detalhar as coordenações necessárias em cada fase do Monitoramento: gerenciamento, auditoria e validação.
- Devem ser atribuídas regras e responsabilidades de Contraineligência, que podem ser complementadas com orientações detalhadas.

5. PRESCRIÇÕES DIVERSAS

- Observações ou ordens específicas de Inteligência não relatadas anteriormente.

Assinatura
COMANDANTE

APÊNDICES

- 1 - RELATÓRIO DE AUDITORIA
- 2 - RELATÓRIO DE VALIDAÇÃO
- 3 - LISTA DE VERIFICAÇÃO (Omitida)

Observações:

- a Lista de Verificação (*checklist*) deverá ser elaborada por grupos de medidas e de acordo com as características da OM; e
- outros anexos poderão ser elaborados, conforme as particularidades da OM.

APÊNDICE 1 AO ANEXO E
RELATÓRIO DE AUDITORIA
(MODELO)

Organização: _____

Local: _____

Data: _____

1. CABEÇALHO

Número: _____	Equipe de Auditoria			Tipo de auditoria		
Local auditado: _____				Presidente	Membro	Membro
Data: _____						
Visto Of Contraineligência _____						
				() Programada () Inopinada () Interna () Solicitada		

2. QUADRO RESUMO DE AUDITORIA (Exemplo)

SEGURANÇA DOS RECURSOS HUMANOS (a)			
Item da Lista de Verificação (b)	Conforme (c)	Não conforme (d)	Oportunidade de melhoria (e)
1) Os integrantes da OM recebem instruções periódicas sobre acidentes na instrução e no serviço?	X		
2) Os integrantes da OM recebem instruções periódicas sobre prevenção de suicídio?		X	1
“n”) De acordo com a Lista de Verificação		X	“n”

OBSERVAÇÕES

(a) Listar os grupos de medidas da Segurança Orgânica.

(b) De acordo com a Lista de Verificação.

(c) Identificar os itens da Lista de Verificação nos quais as deficiências foram sanadas.

(d) Identificar os itens da Lista de Verificação nos quais as deficiências não foram sanadas.

(e) Numerar, de acordo com a sequência de sugestões para atender ao item da Lista de Verificação. Lançar os achados de auditoria (Oportunidade de Melhoria) que indiquem a necessidade de implementação ou aperfeiçoamento na OM no item 4 deste apêndice, em forma de relatório.

3. PARTE EXPOSITIVA

a. Metodologia

- Deverá ser abordada a metodologia utilizada na auditoria, alcance e limitação, escopo da auditoria, duração e espaço amostral.

4. GRUPO DE MEDIDAS DE SEGURANÇA ORGÂNICA

a. Segurança dos Recursos Humanos

1) Pontos Fortes

- Apresentar os achados de auditoria (rotinas, processos, procedimentos, equipamentos, instalações etc.) que indiquem a existência de pontos fortes na OM.

2) Oportunidades de Melhoria

- Apresentar os achados de auditoria (rotinas, processos, procedimentos, equipamentos, instalações etc.) que indiquem a necessidade de implementação ou aperfeiçoamento na OM, de acordo com a numeração lançada no Quadro Resumo de Auditoria.

b. Segurança do Material

1) Pontos Fortes

2) Oportunidades de Melhoria

c. Segurança da Informação

1) Pontos Fortes

2) Oportunidades de Melhoria

d. Segurança das Áreas e Instalações

1) Pontos Fortes

2) Oportunidades de Melhoria

5. CONCLUSÃO

- Apresentar a síntese dos principais aspectos de Segurança Orgânica identificados na auditoria, concluindo sobre o seu impacto para a OM.

Assinatura
PRESIDENTE DA EQUIPE

APÊNDICE 2 AO ANEXO E
RELATÓRIO DE VALIDAÇÃO
(MODELO)

1. Data:
2. Tipo de Auditoria realizada: programada, inopinada ou solicitada.
3. Seções envolvidas na Auditoria:
4. Aspectos levantados na Auditoria que apresentam não conformidade:

ASPECTO	NÃO CONFORMIDADE LEVANTADA (a)	MOTIVO	OBSERVAÇÕES (b)

(a) O validador deverá expor a concordância ou não com os achados de auditoria considerados não conforme.

(b) O validador deverá apresentar justificativa sobre cada item de que discordar.

5. Propostas

- Propor as medidas a serem implementadas para a solução dos problemas verificados na auditoria.
- Propor prazos e indicar responsáveis para a solução dos itens apontados.

Assinatura
VALIDADOR

DESPACHO DO COMANDANTE

Local e Data

Assinatura
COMANDANTE

Publicado em Boletim de Acesso Restrito em: _____

ANEXO F**MONTAGEM DE LISTAS DE VERIFICAÇÃO****1. CONCEITO**

a. São questionários elaborados com a finalidade de verificar se as normas, diretrizes e os procedimentos de segurança estabelecidos estão sendo eficientes e eficazes na aferição da situação da Contraineligência da OM.

b. São elaboradas de forma didática e abrangem todos os grupos de medidas de Segurança Orgânica, constituindo uma base para as equipes de avaliação, auditoria e validação, não tendo como objetivo esgotar o assunto.

2. CONSIDERAÇÕES GERAIS

a. As Listas de Verificação (*checklist*), a princípio, não deverão ser classificadas, a fim de poderem ser afixadas em locais de fácil acesso e de grande circulação da OM, bem como ter seus trechos reproduzidos nos materiais gráficos a serem confeccionados.

b. As ferramentas apresentadas neste anexo são sugestões para facilitar a montagem de listas de verificação. Têm como pré-requisito a necessidade de se conhecer o ator hostil, sua motivação e capacidade de atuar, bem como as deficiências do sistema em estudo.

3. FERRAMENTA 5W1H

O emprego dessa ferramenta pode ser definido por intermédio das seguintes perguntas: O quê? (*what*), onde? (*where*), quando? (*when*), quem? (*who*), por quê? (*why*), como? (*how*).

a. O quê?

Consiste em enfocar vulnerabilidades como um todo, com o objetivo de identificar ameaças ou deficiências que envolvem o problema.

b. Onde?

É usado para limitar a área onde foi identificada a deficiência no processo ou onde o ator hostil poderá investir para se beneficiar.

c. Quando?

É usado para definir o momento adequado para a verificação do resultado das medidas adotadas para sanar as deficiências ou criar barreiras ao ator hostil.

d. Quem?

Identifica os responsáveis por colocar em execução as medidas para solução da deficiência identificada.

e. Por quê?

É a finalidade da ação de proteção dos ativos.

f. Como?

Define quais são as medidas a serem postas em prática para melhorar ou padronizar o processo em estudo.

4. BRAINSTORMING

a. É uma técnica de trabalho em grupo na qual se busca produzir o máximo de soluções possíveis para um determinado problema: um grupo relacionado de deficiências, de ameaças ou de vulnerabilidades.

b. Serve para estimular a imaginação e fazer surgir ideias, o que seria mais difícil, se o trabalho fosse realizado individualmente.

c. É importante ressaltar as seguintes regras básicas:

- 1) as ideias devem ser citadas com o máximo de espontaneidade;
- 2) todas as ideias são de interesse, pois, às vezes, as ideias que parecem estranhas para o caso em estudo podem possuir valor;
- 3) nenhuma ideia deve ser contestada ou debatida, durante a atividade;
- 4) a ideia a ser apresentada, decorrente de outra já exposta, terá prioridade; e
- 5) provavelmente, quanto maior a quantidade de ideias levantadas, o resultado será melhor.

5. HISTÓRICO DE ACIDENTES E INCIDENTES OCORRIDOS

- O histórico da OM sobre acidentes e incidentes, mesmo os que não tenham gerado danos aos seus ativos, pode ser utilizado como base para a elaboração de uma lista de verificação.

ANEXO G**PROCEDIMENTOS DE MESAS E TELAS LIMPAS**

1. A OM deve considerar a adoção de procedimentos de mesas de trabalho limpas para papéis e mídias removíveis e de telas de monitores de meios informatizados limpa, de forma a reduzir riscos de acesso não autorizado, perdas e danos à informação.
2. Os procedimentos devem levar em consideração as classificações da segurança da informação, os riscos correspondentes e os aspectos culturais da OM.
3. As informações deixadas em mesas de trabalho são alvos prováveis de danos ou destruição em eventos tais como incêndio, inundações ou explosões.
4. Recomenda-se que, entre outros, os seguintes controles sejam considerados:
 - a) onde e quando apropriado, é necessário que papéis e mídias sejam guardados de forma segura, em mobiliário adequado, durante os momentos em que não estiverem sendo utilizados;
 - b) computadores pessoais, terminais de computador e impressoras não devem ser deixados ligados sem a presença do usuário e devem ser protegidos por senhas, chaves ou outros controles quando não estiverem em uso;
 - c) pontos de recepção e envio de correspondências, sem a presença do usuário, devem ser protegidos;
 - d) copiadoras devem ser travadas (ou, de alguma forma, protegidas contra o uso não autorizado) fora do horário normal de trabalho; e
 - e) sempre que possível, o usuário deve usar senha para imprimir qualquer documento contendo dados ou informações sensíveis, os quais devem ser retirados da impressora imediatamente.

ANEXO H**DECÁLOGO DA CONTRAINTELIGÊNCIA****1. ESTABELEÇA DIRETRIZES, NORMAS E PROCEDIMENTOS**

- Estabeleça, difunda e fiscalize a execução das diretrizes, normas e procedimentos relacionados à Contrainteligência, que devem ser exequíveis, claros, precisos e simples. Assegure-se que essas orientações contribuam para a salvaguarda dos recursos humanos, da informação, do material e das áreas e instalações.

2. ESTIMULE A COMUNICAÇÃO SOBRE AMEAÇA

- Conscientize e motive os integrantes da OM a informar seus superiores imediatos acerca de possíveis ameaças, pois cada um deles é um sensor de Contrainteligência.

3. REALIZE TREINAMENTOS CONSTANTES

- Mantenha a OM treinada para adotar medidas preventivas de Contrainteligência e responder com efetividade às ameaças.

4. GERENCIE OS RISCOS

- Oriente, controle e estimule os trabalhos de identificação, análise, avaliação e tratamento de riscos na OM.

5. MANTENHA O PLANO DE SEGURANÇA ORGÂNICA ATUALIZADO

- Monitore o PDCl e mantenha atualizados o PSO da OM e seus anexos.

6. ATUE, NA SEGURANÇA ORGÂNICA, COM FOCO NA SALVAGUARDA DOS ATIVOS DA OM

- Levante as deficiências passíveis de serem exploradas por ameaças de qualquer natureza contra ativos da OM e adote medidas para a proteção desses ativos.

7. TENHA EM MENTE QUE O FOCO DA SEGURANÇA ATIVA DEVE ESTAR NA AMEAÇA

- Colabore com os especialistas em Segurança Ativa para detectar, identificar, avaliar, explorar e neutralizar ameaças.

8. RESPEITE E FAÇA RESPEITAR A COMPARTIMENTAÇÃO

- Assegure-se de que o acesso a dados e informações somente seja permitido a quem tenha necessidade de conhecer.

9. ESTIMULE A POSTURA DE PREVENÇÃO

- Conscientize os integrantes da OM sobre a importância de prevenir danos aos ativos da Organização. Antecipe-se aos problemas.

10. FIQUE ATENTO

- Não descuide das medidas de Contrainteligência. Assegure-se de que os integrantes da OM também se mantenham alerta quanto a eventuais ameaças.

GLOSSÁRIO

PARTE I - ABREVIATURAS E SIGLAS

A

Abreviaturas/Siglas	Significado
ACIM	Ações Contra Instalações Militares
ARP	Aeronave Remotamente Pilotada
ATCI	Assessoria Técnica de Contraineligência

F

Abreviaturas/Siglas	Significado
Fig	Figura

I

Abreviaturas/Siglas	Significado
IGSAS	Instruções Gerais para Salvaguarda de Assuntos Sigilosos

M

Abreviaturas/Siglas	Significado
MEM	Material de Emprego Militar
MTIC	Meios de Tecnologia da Informação e Comunicações

N

Abreviaturas/Siglas	Significado
Nr	Número

O

Abreviaturas/Siglas	Significado
OAJU	Outros aspectos julgados úteis
OM	Organização Militar
ORCRIM	Organização criminosa
OSO	Oficial de Segurança Orgânica
OSP	Órgão(s) de Segurança Pública

P

Abreviaturas/Siglas	Significado
PDCI	Processo de Desenvolvimento da Contraineligência
PSO	Plano de Segurança Orgânica

S

Abreviaturas/Siglas	Significado
SIEx	Sistema de Inteligência do Exército

T

Abreviaturas/Siglas	Significado
Tab	Tabela
TCI	Termo de Classificação da Informação
TCMS	Termos de Compromisso e Manutenção de Sigilo
TI	Tecnologia da Informação

PARTE II – TERMOS E DEFINIÇÕES

Ação hostil - ação, intencional ou não, que possa causar danos aos ativos do Exército Brasileiro.

Ameaça - conjunção de ator, motivação e capacidade de realizar ação hostil, real ou potencial, com possibilidade de, por intermédio da exploração de deficiências, comprometer as informações, afetar o material, o pessoal e seus valores, bem como as áreas e instalações, podendo causar danos ao Exército Brasileiro.

Análise de Riscos - estabelecimento da probabilidade de o risco ocorrer e de seu impacto nos ativos da Organização Militar.

Antiterrorismo - conjunto de atividades e medidas defensivas de caráter eminentemente preventivo, destinado a dissuadir indivíduos ou grupos (nacionais, estrangeiros ou transnacionais) que tenham a intenção e capacidade de empregar táticas, técnicas e procedimentos típicos de organizações terroristas. Destina-se, também, a detectar e identificar ameaças terroristas reais ou potenciais e a impedir suas ações.

Assessoria Técnica de Contrainteligência - assessoria pela qual são orientados os trabalhos de Segurança Orgânica da OM, conforme os grupos de medidas, sendo realizada por meio de visitas de orientação regulares ou inopinadas, por iniciativa própria do Escalão Superior, ou por solicitação da OM considerada.

Autenticação - declaração de que um documento original é autêntico, ou que uma cópia reproduz fielmente o original, feita por uma pessoa jurídica com autoridade para tal (servidor público, notário ou autoridade certificadora) em um determinado momento.

Autenticação de documento - processo utilizado para confirmar ou garantir ao usuário a identidade de uma pessoa ou organização, garantindo a fidelidade da fonte e confirmando a procedência da documentação.

Autenticação de mensagem - técnica utilizada para garantir a integridade de mensagens enviadas, detectando modificações não autorizadas ou corrupção do seu conteúdo.

Avaliação de Riscos - interação entre a probabilidade e o impacto, estabelecendo-se o valor e o nível de risco, que tem por finalidade auxiliar na tomada de decisão para o tratamento de riscos.

Barreira - obstáculo de qualquer natureza, instalado para impedir o ingresso de pessoas não autorizadas às áreas de acesso restrito e permitir o controle da circulação das pessoas que possuam autorização para tal.

Capacidade de agir - potencial de um ator para executar determinada ação.

Classificação - o ato de se atribuir grau de sigilo à informação que requeira medidas especiais de salvaguarda e, por consequência, aos seus suportes.

Código do risco - número que identifica o risco.

Compartimentação - restrição do acesso com base na necessidade de conhecer.

Confidencialidade - (sigilo) - garantia de que o conteúdo da informação só é acessível e interpretável por quem possuir autorização para a ela ter acesso.

Contrainteligência - ramo da Atividade de Inteligência Militar voltado para prevenir, detectar, identificar, avaliar, obstruir, explorar e neutralizar a atuação da Inteligência adversa (hostil) e as ações de qualquer natureza que possam se constituir em ameaças à salvaguarda de dados, conhecimentos, áreas, instalações, pessoas e meios que o Exército Brasileiro tenha interesse de preservar.

Contrainteligência Interna - grupo de medidas da Segurança Ativa destinado a acompanhar as ações dos integrantes do público interno de modo a detectar, identificar, avaliar, explorar e neutralizar ameaças que possam gerar riscos para os valores, os deveres e a ética militar no Exército.

Contra-ações psicológicas - grupo de medidas da Segurança Ativa destinado a detectar, identificar, avaliar, explorar e neutralizar a ação psicológica hostil, em especial a propaganda, que possa causar prejuízos e danos ao Exército Brasileiro.

Contraespionagem - grupo de medidas da Segurança Ativa destinado a detectar, identificar, avaliar, explorar e neutralizar ações de espionagem.

Contrapropaganda - conjunto de ações implementadas no sentido de prevenir, neutralizar ou minimizar os efeitos da propaganda inimiga, adversa ou oponente sobre o público-alvo.

Contrassabotagem - grupo de medidas da Segurança Ativa destinado a detectar, identificar, avaliar, explorar e neutralizar atos de sabotagem contra a Instituição, pessoas e seus valores, documentos, materiais, equipamentos e instalações que ao Exército Brasileiro interessem preservar.

Contraterrorismo - grupo de medidas voltado a contribuir para a detecção, identificação, avaliação e neutralização de atos e ameaças terroristas.

Comprometimento - perda de segurança resultante do acesso não autorizado.

Criptografia - técnica utilizada para tornar ininteligível o texto da mensagem, mediante o emprego de cifras e chaves apoiadas em um algoritmo de transformação.

Desinformação - 1. Técnica especializada utilizada para iludir ou confundir um centro decisor, por meio da manipulação planejada de informações falsas ou verdadeiras, visando, intencionalmente, a induzi-lo a erro de avaliação. 2. Fenômeno decorrente de acentuadas deficiências em exatidão, amplitude e/ou aprofundamento das informações disponíveis aos decisores e ao público em geral. A desinformação leva a uma percepção significativamente equivocada, incompleta ou distorcida da realidade e, por fim, promove decisões e comportamentos inadequados às circunstâncias.

Disponibilidade - garantia de que o conteúdo da informação esteja disponível para quem possuir autorização ou credencial de segurança, sempre que houver necessidade.

Drone - veículo aéreo, terrestre ou marítimo que é pilotado remotamente ou dotado de navegação autônoma.

Espionagem - ação realizada por pessoal, vinculado ou não a serviço de Inteligência, visando à obtenção de conhecimento, dado sigiloso, documento ou material para beneficiar Estados, grupos de países, organizações, facções, empresas, personalidades ou indivíduos.

Exame de Situação - processo sistemático de planejamento detalhado que visa a dar uma sequência lógica e ordenada aos diversos fatores que envolvem o processo decisório relacionado à Contrainteligência.

Informação classificada - informação sigilosa em poder do órgão ou entidade pública, que recebeu de autoridade competente classificação no grau de sigilo ultrassecreto, secreto ou reservado devido ao seu teor, e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado.

Informação de acesso restrito - informação que, desclassificada ou não sendo passível de receber classificação sigilosa, por sua utilização ou finalidade, demanda medidas especiais de proteção.

Informação sensível - informação classificada, de acesso restrito ou ostensiva que, em decorrência de sua natureza ou conteúdo, necessite de medidas de proteção.

Informação sigilosa - informação submetida, temporariamente, à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado ou por ser abrangida pelas demais hipóteses legais de sigilo.

Integridade - garantia de que o conteúdo original da informação não seja modificado; é a certeza de que a exatidão e a inteireza estejam salvaguardadas.

Irretratabilidade (não repúdio) - garantia de que, num processo de envio e recebimento de informações, qualquer participante originador ou destinatário de informação não possa, em um momento posterior, negar a respectiva atuação.

Malwares - programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Eles podem ser vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia (*trojan horse*), *rootkit* ransomware, entre outros.

Medidas de Contingência - medidas estabelecidas com o objetivo de prover meios e procedimentos alternativos, diante de situações que ameacem a Segurança Orgânica, com o intuito de assegurar a continuidade ou restabelecer o funcionamento dos ativos afetados.

Motivação - estado interno que resulta de uma necessidade do ator, dirigindo

o comportamento humano para a satisfação dessa necessidade.

Necessidade de conhecer - condição pessoal, inerente ao efetivo exercício de cargo, da função, do emprego ou da atividade, indispensável para que uma pessoa tenha acesso à informação sensível.

Público Interno - público constituído pelos militares da ativa e inativos, ex-combatentes e servidores civis, todos do Exército, bem como, naquilo que couber, seus dependentes e os alunos dos Colégios Militares.

Público Externo - público constituído pelas pessoas, grupos de pessoas ou organizações não incluídos no público interno.

Phishing - e-mails que parecem ser enviados por pessoas conhecidas ou por organizações legítimas, normalmente visando a induzir o usuário a clicar em um arquivo malicioso anexado ou direcioná-lo a um site falso, também malicioso.

Plano de Controle de Danos - plano composto de medidas que devem ser adotadas para verificar, em caso de dano, o comprometimento dos ativos que deveriam ter sido protegidos e suas consequências para a imagem do Exército.

Plano de Conscientização - plano que regula as ações voltadas para obter e manter atitudes favoráveis ao PDCI pelos integrantes da OM.

Plano de Monitoramento do PDCI - plano estabelecido com a finalidade de controlar permanentemente os planos que compõem o PDCI, identificando oportunidades de melhoria, bem como realimentando-o.

Plano de Treinamento Continuado - plano que regula o desenvolvimento da instrução e do adestramento dos integrantes da OM, visando à execução das ações previstas no PDCI.

Plano de Segurança Orgânica - plano que consubstancia as medidas necessárias à implementação da Segurança Orgânica a serem adotadas pela OM.

Processo de Desenvolvimento da Contrainteligência - conjunto de atividades contínuas de Contrainteligência destinadas a planejar, controlar e otimizar as medidas de segurança para proteger pessoas, informações, materiais, áreas e instalações (ativos do Exército), por meio do estabelecimento e da manutenção de medidas de segurança eficientes e eficazes, além do desenvolvimento da mentalidade de Contrainteligência.

Propaganda - difusão de qualquer informação, ideia, doutrina ou apelo especial, visando a gerar emoções, influenciar atitudes e opiniões ou dirigir o comportamento de indivíduos ou grupos, a fim de beneficiar, direta ou indiretamente, quem a promoveu.

Ransomware - tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

Rootkit - conjunto de programas e técnicas que permitem esconder e assegurar a

presença de um invasor ou de outro código malicioso em um computador comprometido, impedindo sua detecção pelo usuário e por mecanismos de segurança.

Sabotagem - qualquer ação sub-reptícia destinada a perturbar, interferir, causar dano, destruir ou comprometer o funcionamento normal de diferentes sistemas nos campos político, econômico, científico-tecnológico, psicossocial e militar.

Segurança Ativa - segmento da Contrainteligência que preconiza a adoção de um conjunto de ações de especialistas, de caráter eminentemente preditivo, destinado a detectar, identificar, avaliar, explorar e neutralizar as ameaças de qualquer natureza, contra o Exército Brasileiro.

Segurança das Áreas e Instalações - grupo de medidas voltadas para os locais em que ocorram atividades humanas, ou nos quais são elaboradas, tratadas, manuseadas ou guardadas informações e materiais, com a finalidade de salvaguardá-los.

Segurança da Informação - grupo de medidas destinado a garantir a disponibilidade, integridade, confidencialidade (sigilo), autenticidade, a irretratabilidade (não repúdio) e atualidade da informação em todo o seu ciclo de vida.

Segurança da Informação na Documentação - subgrupo de medidas aplicadas à documentação, destinadas a evitar o seu comprometimento, visando à salvaguarda de dados, informações ou conhecimentos, de caráter sigiloso ou não, que devam ser protegidos.

Segurança da Informação nas Áreas e Instalações - subgrupo de medidas voltadas para preservar as informações sobre áreas e instalações pertencentes ou de interesse do Exército.

Segurança da Informação no Material - subgrupo de medidas voltadas para proteger as informações contidas em determinados materiais.

Segurança da Informação nos Meios de Tecnologia da Informação e Comunicações - subgrupo de medidas destinadas a salvaguardar as informações, bem como a integridade dos sistemas e meios de TIC do Exército.

Segurança da Informação no Pessoal - consiste no subgrupo de medidas destinadas a assegurar comportamentos, no público interno, adequados à proteção de dados e informações de natureza institucional.

Segurança do Material - grupo de medidas voltadas à proteção do material do EB, de forma direta ou indireta.

Segurança Orgânica - segmento da Contrainteligência que preconiza a adoção de um conjunto de medidas destinado a prevenir e obstruir possíveis ameaças de qualquer natureza dirigidas contra pessoas, dados, informações, materiais, áreas e instalações.

Segurança dos Recursos Humanos - consiste no grupo de medidas destinadas a preservar a integridade física e moral dos recursos humanos.

Suportes da informação - pessoas, documentos, materiais, MTIC, áreas e instalações que contenham, utilizem ou veiculem a informação.

Spyware - programa projetado para monitorar as atividades de um sistema, coletando hábitos *online*, histórico de navegação ou informações pessoais (como senhas, por exemplo), enviando as informações coletadas para terceiros.

Vírus - programas que se propagam inserindo cópias de si mesmos, tornando-se parte de outros programas e arquivos.

Vazamento - divulgação não autorizada de informação sensível.

Vulnerabilidade - deficiência que, ao ser explorada pela ameaça, pode causar incidentes de segurança e gerar impactos negativos para o Exército Brasileiro.

Worm - programa que envia cópias de si mesmo de computador para computador. Diferentemente do vírus, o *worm* não precisa ser executado pelo usuário, propagando-se pela execução automática de suas cópias e explorando deficiências existentes em programas instalados nos computadores.

REFERÊNCIAS

- BRASIL. Presidência da República. **Política Nacional de Inteligência**. Brasília, DF, 2016.
- _____. **Estratégia Nacional de Inteligência**. Brasília, DF, 2017.
- _____. Gabinete de Segurança Institucional da Presidência da República. **Doutrina Nacional da Atividade de Inteligência**. Brasília, DF, 2016.
- _____. Ministério da Defesa. **Doutrina de Inteligência de Defesa. MD52-N-01**. Brasília, DF, 2005.
- _____. **Glossário das Forças Armadas. MD35-G-01**. 4. ed. Brasília, DF, 2007.
- _____. **Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas. MD33-M-02**. 3. ed. Brasília, DF, 2008.
- _____. Exército Brasileiro. Comando do Exército. **Instruções Gerais para as Publicações Padronizadas do Exército. EB10-IG-01.002**. Brasília, DF, 2011.
- _____. **Instruções Gerais para a Salvaguarda de Assuntos Sigilosos. EB10-IG-01.011**, 1. ed. Brasília, DF, 2014.
- _____. Exército Brasileiro. Estado-Maior do Exército. **Manual de Campanha Contra Inteligência. C 30-3**. 2.ed. Brasília, DF, 2009.
- _____. **Vade-Mécum de Inteligência Militar**. Brasília, DF, 2011.
- _____. **Manual de Campanha Inteligência. EB20-MC-10.207**. Brasília, DF, 2015.
- _____. **Manual de Fundamentos Inteligência Militar Terrestre. EB20-MF-10.107**. 2. ed. Brasília, DF, 2015.
- _____. **Manual de Campanha Proteção. EB20-MC-10.208**. 1. ed. Brasília, DF, 2015.
- _____. **Metodologia da Política de Gestão de Riscos do Exército Brasileiro. EB20-D-07.089**, 1. ed. Brasília, DF, 2017.
- _____. Exército Brasileiro. Comando de Operações Terrestres. **Manual de Campanha Planejamento e Emprego da Inteligência Militar. EB70-MC-10.307**. 1. ed. Brasília, DF, 2016.
- _____. **Manual de Campanha Operações Especiais. EB70-MC-10.212**. 1. ed. Brasília, DF, 2017.
- _____. **Glossário de Termos e Expressões para Uso no Exército. EB20-MF-03.109**, 5. ed. Brasília, DF, 2018.

COMANDO DE OPERAÇÕES TERRESTRES
CENTRO DE DOCTRINA DO EXÉRCITO
Brasília, DF, 26 de julho de 2019
www.cdoutex.eb.mil.br